PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-286989
(43)Date of publication of application : 13.10.2005

(51)Int.Cl. H04L 12/28
H04L 12/56

(21)Application number : 2004-250816
(22)Date of filing : 30.08.2004

(71)Applicant : NTT DOCOMO INC
(72)Inventor : HAGIWARA JUNICHIRO
AOKI HIDENORI
UMEDA SEISHI

(30)Priority
Priority number : 2004058072 Priority date : 02.03.2004 Priority country : JP

(54) COMMUNICATION TERMINAL AND AD HOC NETWORK ROUT CONTROLLING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a rout controlling methodetc. for preventing a risk of believing false rout control informationand for concealing address informationetc. of a transmission reception terminal and a relay terminal as much as possible in an ad hoc network.
SOLUTION: A communication terminal capable of generating an ad hoc network route is configured by a transmitting receiving unit for performing a communication with other communication terminala route request generating unit for generating a route requesting message for requesting generation of an ad hoc network routean address storing unit for storing an address of a self terminal and an address of a reception terminala random number generating unit for generating a random numbera certificate publishing unit for publishing a certificate of the self terminala digital signature producing unit for producing a digital signature of the self terminaland a controlling unit for transmitting and receiving data configured from an address of the self terminalan address of the reception terminala random numbera certificateand a digital signature by adding to the route requesting message via the transmitting receiving unit in response to an ad hoc network protocol.

CLAIMS

[Claim(s)]

[Claim 1]

It is a communication terminal which has a route request generating part which generates a route request message which requires generation of a transmission and reception section which generation of an ad hoc network course is possibleand performs communication with other communication terminalsand an ad hoc network course. :

An address storage section which memorizes an address of a self-terminaland an address of a receiving terminal;

A random number generation part which generates a random number;

A certificate issue section which publishes a certificate of a self-terminal;

A digital signature preparing part which creates a digital signature of a self-terminal;

A control section which transmits and receives data which added an address of a self-terminalan address of a receiving terminalthe aforementioned random numbera certificateand a digital signature to said route request messageand constituted them according to an ad hoc network protocol via said transmission and reception section;

A communication terminal ** constituted.

[Claim 2]

It is the communication terminal according to claim 1and is a pan. :

A secret key treating part which creates a secret key and enciphers said at least some of data; it reaches.

Operation part which decodes received encrypted data;

A communication terminal ** constituted.

[Claim 3]

It is an ad hoc path control method for generating an ad hoc network among two or more communication terminals. :

A stage which carries out broadcast transmission of the data which added and constituted a transmit-terminal addressa receiving terminal addressand a transmit-terminal digital signature to an ad hoc route request signal in a transmit terminal;

A stage which attests a transmit-terminal digital signature transmitted from a transmit terminal in a relay terminaland adds and carries out broadcast transfer of a relay terminal address and the relay terminal digital signature to said ad hoc route request signal;

A stage which attests said relay terminal digital signature and said transmit-terminal digital signature in a receiving terminal; it reaches.

A stage which addresses an ad hoc course reply signal which added and constituted a receiving terminal digital signature to said received data in said receiving terminal to said transmit terminaland transmits;

An ad hoc path control method ** constituted.
[Claim 4]
It is an ad hoc path control method for generating an ad hoc network among two or more communication terminals. :
A stage of data which added and constituted a transmit-terminal address and a receiving terminal address to an ad hoc route request signal in a transmit terminal which enciphers using a public key of a receiving terminal in part at leastand carries out broadcast transmission of said data;
A stage which adds and carries out broadcast transfer of the relay terminal address to said ad hoc route request signal in a relay terminal;
A stage which addresses an ad hoc course reply signal which added said received data in a receiving terminal to said transmit terminaland transmits;
An ad hoc path control method ** constituted.
[Claim 5]
An ad hoc path control method which is the ad hoc path control method according to claim 3and is characterized by having further a stage where said receiving terminal decrypts said received data in an attestation stage in the aforementioned receiving terminal using a self secret key.
[Claim 6]
An ad hoc path control method which is the ad hoc path control method according to claim 4and is characterized by what said transmit terminal determines a session key and it has the stage of performing hybrid encryption using the session key for in an encryption stage in the aforementioned transmit terminal.
[Claim 7]
An ad hoc path control method which is an ad hoc path control method given in any of the above-mentioned claim they areand is characterized by having further the stage of concealing the aforementioned relay terminal address.
[Claim 8]
An ad hoc path control method which is the ad hoc path control method according to claim 7and is characterized by a stage of concealing the aforementioned relay terminal address comprising a stage of concealing information on an upstream relay terminal using a part of information on a relay terminal.
[Claim 9]
An ad hoc path control method which is an ad hoc path control method given in any of the above-mentioned claim they areand is characterized by having further a stage which inserts a dummy address into said data.
[Claim 10]
An ad hoc path control method which is an ad hoc path control method given in any of the above-mentioned claim they areand is characterized by having further a stage which inserts straw-man padding into said data.
[Claim 11]

An ad hoc network system which contains the communication terminal according to claim 1 or 2 as a transmit terminaland contains a relay terminal and a receiving terminal further.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[Field of the Invention]
[0001]
Especially this invention relates to the ad hoc network path control method which performs attestation and processing for privacy protectionand the communication terminal for it about an ad hoc network path control method and the communication terminal for it.
[Background of the Invention]
[0002]
There is demand of connecting with a mobile radio communication network in connection with a huge expansion and the diversity of mobile communications demand from the mobile communication terminal in the exterior of the field which a mobile communications base station covers. From the direct one hop connection with a base station from the mobile communication terminal outside the cover region of a mobile communications base station being impossible. The method of using for a base station the wireless ad hoc network which makes multi-hop connection is proposed via other mobile communication terminals and simple relay stations installed temporarily. That isa wireless ad hoc network is a wireless network temporarily built by the personal digital assistant which a user usesthe simple relay station installed temporarilyetc. (refer to drawing 1). Each mobile communication terminal and a simple relay station build in an ad hoc routing protocoland spontaneous information is transmitted and received between each terminal according to thisand they constitute an ad hoc network. Since information will be received by various terminalsit is important to secure security and privacy in an ad hoc network.
[0003]
As an example of an ad hoc networkwhen the routing demand from a terminal arisesthere is a DSR (Dynamic Source Routing) method which generates a course. In a DSR methoda transmit terminal can send data using the course by getting to know the address of all the terminals (node) on the course to a receiving terminal. Since the terminal (node) which relays data can know the next destination using the channel information transmitteda relay terminal does not need to have channel information and it can be managed with comparatively light processing. By using an ad hoc networkit becomes possible to provide cellular communications servicean Internet access serviceetc. also to the mobile communication terminal out of the

communications area which a mobile radio communication network provides. In such a communication configurationit works as a component of an ad hoc network and the both sides of a mobile radio communication networkand the communication terminal which bears mediation of the channel from an ad hoc network to a mobile radio communication network is called a gateway terminal (16 references of drawing 1). Heresince the gateway terminal D is an another name of the communication terminal which is carrying out direct continuation to the mobile radio communication networkarbitrary communication terminals can turn into the gateway terminal D. When the gateway terminal D moves out of the area which a mobile radio communication network providesit does not get used to a gateway terminal any longerbut becomes a mere mobile communication terminal.

[0004]

An ad hoc network is constituted as shownfor example in drawing 1. Although the example of mobile radio communication explainsan ad hoc network is not restricted to radiobut is useful also in a wire communication. The moving terminal S (12) forms an ad hoc network according to an ad hoc path control protocol. It is connected to the gateway terminal D (16) via the relay terminal T1 (14) and the relay terminal T2 (15)and the mobile communication terminal S (12) constitutes the ad hoc network from an example of a graphic display. Since the gateway terminal D (16) is in the area which the base station B (18) coversit can connect with the base station B (18) via the gateway terminal D (16)and the moving terminal S (12) can receive the service from there (refer to patent documents 1).

[0005]

Hereit is IETF (for the purpose of The Internet Engineering Task Forceand the better architecture and the smooth operation of the Internet). Standardization of the Internet. The outline of the conventional example of the path control in DSR (Dynamic Source Routing) currently examined by MANET (Mobile Ad-hoc Networks) WG (task force) of the organization which is developing the volunteer activity at the center is shown in drawing 2 and drawing 3.

[0006]

The procedure of the conventional course establishment is explained referring to drawing 2 and drawing 3. Although the transmit terminal S (Source) shown in drawing 2 and drawing 3 is explained as a thing equivalent to the moving terminal S of drawing 1it may not be restricted to thisbut a gateway terminal may be sufficient as itand they may be other moving terminals. Although the receiving terminal D (Destination) shown in drawing 2 and drawing 3 is explained as a thing equivalent to the gateway terminal D of drawing 1it may not be restricted to this but may be a moving terminal. Although the relay terminal T (Transmitter) shown in drawing 2 and drawing 3T1and T2 are explained as a thing equivalent to the relay terminals 14 and 15 of drawing 1they are not restricted to this. Since the relay terminal T1 of drawing 3 and T2 have composition and the the same functionin drawing 2the one relay terminal T represents

and is shown.

[0007]

When the transmit terminal S starts communication with the receiving terminal Drequest/reply generating part 222The signal of RREQ (Route REQuest) which is a control message for requiring generation of an ad hoc network course is generatedand the transmission and reception section 226 carries out broadcast transmission of the RREQ to a network. Address ADD_S of a transmit terminal and address ADD_D of a receiving terminal are read from the address storage section 227are added to RREQand are transmitted together. An address may be an IP addressfor example. The information which restricts the hop number which carries out re transfer may also be included in control message PREQ.

[0008]

The relay terminal T1 which received control message RREQ by the transmission and reception section 246If it turns out that its address ADD_{T1} memorized in the address storage section 247 is compared with address ADD_D which receivedand there is nothing at addressing to itselfits address ADD_{T1} will be added and RREQ will be transmitted by broadcasting.

[0009]

The transmission processing as the terminal T1 that the relay terminal T2 is also the same is performed.

[0010]

The receiving terminal D which received control message RREQ. adding what copied relay address information to a control message called RREP (Route REPly)if their address and ADD_D which were memorized in the address storage section 267 are compared and it turns out that it is addressing to itself -- a unicast -- the transmit terminal S -- it sends a reply.

[0011]

The relay terminal T2 which received RREP will transmit this signal by a unicastif its address is discovered to a relay address list.

[0012]

The processing as the terminal T2 that the relay terminal T1 is also the same is performed.

[0013]

From the combination of address information ADD_S and $ADD_D$the transmit terminal S which received RREP can recognize that this signal is the response to RREQ which he transmitted beforeand can know relay path information (S->T1->T2->D).

[Patent documents 1] JP2003-230167A

[Description of the Invention]

[Problem(s) to be Solved by the Invention]

[0014]

Howeverin the DSR ad hoc network in conventional technologysince attestation of

RREQ which is a path control signalor RREP was omittedthere was a danger of believing the mistaken path control information. Since transceiver person informationthe address information of a relay nodeetc. were stored in a header in the state where anyone can reada third party is able to specify a transceiver personand there were a problem of privacyetc.

[0015]

ThenSUBJECT of this invention is providing the path control method etc. which can avoid the danger of believing the mistaken path control information by performing attestation of RREQ and RREP in an ad hoc network.

[0016]

It is providing the path control method etc. which can improve the privacy of the sender receiver terminal to a third party by concealing the address information of a sender receiver terminal or a relay terminaletc. as much as possible.

[Means for Solving the Problem]

[0017]

Generation of an ad hoc network course according to one feature of this invention for attaining above-mentioned SUBJECT is possibleA communication terminal which has a route request generating part which generates a route request message which requires generation of a transmission and reception section which performs communication with other communication terminalsand an ad hoc network courseA digital signature preparing part which creates a digital signature of a certificate issue section; self-terminal which publishes a certificate of a random number generation part; self-terminal which generates an address storage section; random number which memorizes an address of a self-terminaland an address of a receiving terminal; according to an ad hoc network protocolIt comprises control-section; which transmits and receives data which added an address of a self-terminalan address of a receiving terminala random numbera certificateand a digital signature to a route request messageand constituted them via a transmission and reception section.

[0018]

Furthersuch a mobile communication terminal may create a secret keyand may have the operation part which decodes secret key treating part; and received encrypted data which encipher at least some data.

[0019]

An ad hoc path control method for generating an ad hoc network among two or more communication terminals according to one feature of this invention for attaining above-mentioned SUBJECTA stage which carries out broadcast transmission of the data which added and constituted a transmit-terminal addressa receiving terminal addressand a transmit-terminal digital signature to an ad hoc route request signal in a transmit terminal; In a relay terminalA stage which attests a transmit-terminal digital signature transmitted from a transmit terminaland adds and carries out broadcast transfer of a relay terminal address and the relay terminal digital signature to an ad

hoc route request signal; In a receiving terminalIn stage; and a receiving terminal which attest a relay terminal digital signature and a transmit–terminal digital signatureit comprises stage; which addresses an ad hoc course reply signal which added and constituted a receiving terminal digital signature to received data to a transmit terminaland transmits.

[Effect of the Invention]

[0020]

If working example of this invention is followedthe danger of believing the mistaken path control information is avoidable by performing attestation of RREQ and RREP. The privacy protection of the sender receiver terminal to a third party can be raised by concealing the address information of a sender receiver terminal or a relay terminaletc. as much as possible.

[Best Mode of Carrying Out the Invention]

[0021]

Hereaftereach working example of this invention is describedreferring to Drawings. Firstthe premise about each working example of this invention is expressed.

[0022]

– By a means of some kindall the nodes (terminal) hold the certificate of route CA (Certificate Authoritycertificate authority)can publish their own certificateand can create a secret key.

[0023]

– By a means of some kindthe address and certificate of a communications partner can be known before a communication start.

[Work example 1]

[0024]

Working example 1 of this invention is described referring to drawing 4 and drawing 5. The moving terminal 400 according to working example of this inventionIt has request/reply generating part 422the control section 424the transmission and reception section 426the address storage section 427the address comparison part 428the random number generation part 430the certificate issue section 440the digital signature preparing part 450the secret key treating part 460the operation part 470and the verification part 480. This composition is not restricted to a transmit terminalbut has composition also with same relay terminal and receiving terminal. This invention is not restricted to mobile radio communicationbut can be applied also to a wire communication.

[0025]

The transmission and reception section 426 carries out broadcast transmission of the route request control message RREQ generated in request/reply generating part 422 to a network.

[0026]

In working example 1in RREQattestation was applied between each hop

(namelybetween the transmit-terminal S-> relay terminal T1 -> relay terminal T2 -> receiving terminals D)and attestation is applied only in between (namelybetween the receiving terminal D-> transmit terminals S) by RREP as shown in drawing 5. It adds shading to a different portion from drawing 3 among drawing 5and it is shown. Nonce shown in drawing 5 means the random number generated in the random number generation part 430. $Cert_X$ means the certificate of the terminal X which a certificate issue section publishes. Sig_X is a digital signature by the terminal X.
It is created by the digital signature preparing part.

[0027]
In DSR of a conventional examplealthough attestation of RREQ and RREP is omittedthese signals are attested in this example. Since every relay node is attested by RREQit is thought by RREP of a reply that attestation of a between is enough.
[0028]
It explains per operation of each terminal below. The random number generation part 430 of the transmit terminal S determines the random number Nonce first. The certificate issue section 440 publishes $Cert_S$. The control section 424 adds Nonce and own certificate $Cert_S$ to control message RREQ. The random number Nonce is added in order to protect a network from a resending attack. The receiving terminal adds a transmit terminal's own certificate to RREQ in order not to necessarily know the information on a transmit terminal. The digital signature preparing part 450 creates own digital signature Sig_S Nonce and for all the fields of the signal RREQ which added certificate $Cert_S$. The transmission and reception section 426 transmits to a network the signal RREQ with which Nonce$Cert_S$and Sig_S were added by broadcasting.
[0029]
The verification part 480 of the relay terminal T1 which received the signal RREQ verifies Nonce contained in the received signal RREQ by a publicly known method. When Nonce is the same as the value of Nonce which received beforeit is recognized as this RREQ being retransmission of messageand cancels. When Nonce is the first value to receivethe verification part 480 verifies digital signature Sig_S of a transmit terminal by a publicly known method using certificate $Cert_S$ added. If satisfactory as a result of verificationit will check that ADD_D is compared with its address and there is nothing at addressing to itself. Nextaddress ADD_{T1} and certificate $Cert_{T1}$ of relay terminal T1 self are added to the received signaland digital signature Sig_{T1} of relay terminal T1 self is created to the whole added signal. $ADD_{T1}Cert_{T1}$and RREQ that added Sig_{T1} are transmitted to a network by broadcasting.
[0030]
The processing as the relay terminal T1 that the relay terminal T2 is also the same is performed. Howeverdigital signature Sig_{T1} of the relay terminal T1 is verified using certificate $Cert_{T1}$ added$ADD_{T2}Cert_{T2}$and Sig_{T2} are added to the RREQ signal received from the relay terminal T1and it transmits to a network by broadcasting.

[0031]
The verification part 480 of the receiving terminal D which received the RREQ signal from the relay terminal T2 verifies Nonce. When Nonce is the same as the value of Nonce which received beforeit is recognized as this RREQ being retransmission of messageand cancels. When Nonce is the first value to receivedigital signature Sig_{T2} of a relay terminal is verified using certificate $Cert_{T2}$ added. ADD_D is compared with its address and it recognizes that it is addressing to itself. Digital signature Sig_{T1} of a relay terminal is verified using certificate $Cert_{T1}$ added. Digital signature Sig_S of a transmit terminal is verified using certificate $Cert_S$ added. The turn of these processings may be changed.
[0032]
The copy of the contents of RREQ is added to the reply control message RREP generated by request/reply generating part of the receiving terminal D. Digital signature Sig_D of the receiving terminal D is created for all the fields of the RREP signal which added the copy of the contents of RREQ. RREP which added Sig_D is transmitted to transmit-terminal S by a unicast.
[0033]
The relay terminal T2 which received the RREP signal from the receiving terminal D verifies Nonce. Since its address ADD_{T2} can be discovered to a relay address listthis signal is transmitted by a unicast as it is.
[0034]
The processing as the relay terminal T2 that the relay terminal T1 is also the same is performed.
[0035]
The verification part 480 of the transmit terminal S which received the RREP signal by the relay terminal T1 course performs the following processingsafter verifying Nonce first. Since its address ADD_S cannot be discovered to a relay address listit is verified whether it is RREP addressed to itself. He recognizes that it is the response to RREQ which transmitted before from the combination of $ADD_S$$ADD_D$Nonce$Cert_S$and Sig_S. Sig_D is verified. Sig for every relay path is verified. That isRREP is transposed to RREQ and Sig_D is removed. After verifying $Sig_{T2}$$ADD_{T2}$$Cert_{T2}$and Sig_{T2} are removed. After verifying $Sig_{T1}$$ADD_{T1}$$Cert_{T1}$and Sig_{T1} are removed. Relay path information (S->T1->T2->D) is become final and conclusive.
[Work example 2]
[0036]
Working example 2 of this invention is described referring to drawing 6 thru/or drawing 10. Although drawing 6 is the same figure as drawing 5it shows the information about S and D which are exposed by the third party by shading. As shown in drawing 6there is a problem that privacy cannot be protectedin working example 1. For examplein the area where a utilizing user is limitedfor round robin of a certificateif $Cert_S$ pullsthere is a danger that the transmit terminal S will become clear.

[0037]
Thenworking example enciphered and concealed for the improvement in privacy protection so that only S and D may understand the shading field of drawing 6 is described. The common key encryption system which is a fundamental cipher system is a method which the receiving terminal D which the transmit terminal S enciphered plaintext data using the common keytransmitted the enciphered dataand received it decrypts using the same common key. From the place whose encryption and decryption are the same processings of an opposite directionit is also called a "symmetrical algorithm." High-speed processing is attained from using the same key as encryption and decryption. Howeverwhen a "common key" leaks to a third partythere is a disadvantageous point that the danger that all subsequent codes will be decoded becomes high.
[0038]
In the example shown in drawing 7a transient address is applied as address ADD_S of the transmit terminal Sand the method which applied public-key-encryption-ization purely is explained to others. A public-key crypto system or an unsymmetrical algorithm is a method using the key which is differentrespectively as the key used for encryptionand a key used for decryption. Key of one of the two open to a partner is called a "public key." A receiving terminal creates a "secret key" and a "public key" in a pair. The direction of a "public key" is exhibited and the "secret key" is kept with the receiving terminal. A transmit terminal obtains the public key of a receiving terminalenciphers plaintext data using the keyand transmits encrypted data. The receiving terminal which received encrypted data decrypts encrypted data using the kept secret key.
[0039]
HereE_X [y] means enciphering the plaintext y using the public key of X. In the transmit terminal S shown in drawing 7address ADD_D of the receiving terminal DCertificate $Cert_S$ and digital signature Sig_S of the transmit terminal S are enciphered by the public key of the receiving terminal D (E_D [ADD_D]E_D [$Cert_S$]E_D [Sig_S]). The receiving terminal D which received these encrypted data is decrypted using the kept secret key. When sending a replydigital signature Sig_D of self is enciphered by the public key of the transmit terminal S (E_S [Sig_D]). Howeverthere are the following problems in this method.
[0040]
1. Since the coding result to the same plaintextssuch as (original RSA)becomes the always same value depending on the algorithm of public key encryptionalthough ADD_D is unknowna "new" address called E_D [ADD_D] is always exposedand the danger of being pursued exists.
[0041]
2. The same danger exists also to a transient address.
[0042]

Thereforethough the same value is encipheredthe powerful measure [direction / where a result different each time was obtained] to disclosure of privacy is done more.

[0043]

Working example 2 which applied the hybrid code as shown in drawing 8 as working example over this problem is described. According to the hybrid cipher systemthe following processings are performed by a sender receiver terminal. Beforehandboth the sender receiver terminal S and D have shared the common key. The receiving terminal D creates a "secret key" and a "public key" in a pair. The direction of a "public key" is exhibited and the "secret key" is kept with the receiving terminal D. The transmit terminal S obtains the public key of the receiving terminal Denciphers a common key using the public keyand sends it to the receiving terminal D. Using the common key which the transmit terminal S encipheredsymmetrical key encryption of plaintext data is performed and encrypted data is transmitted. The receiving terminal D which received the common key enciphered by the public key and encrypted data decrypts an encrypted common key using the kept secret key. Encrypted data is restored using the decrypted common key. In order for the plaintext data itself to perform encryption/decryption with a common cipher system with a quick speedhigh-speed processing speed is obtained. In order to improve confidentialityit is also possible to change the above-mentioned common key for every session. In that casethe transmit terminal S performs symmetrical key encryption of data using a disposable common key (referred to as Session Key) for every sessionenciphers Session Key by a public keyand notifies to the receiving terminal D.

[0044]

In working example shown in drawing 8a transient address is applied to transmit-terminal address $ADD_S$and a hybrid code is applied to others. Belowit explains focusing on different processing from drawing 3.

[0045]

The random number generation part 430 (refer to drawing 4) of the transmit terminal S determines transient address ADD_S of a transmit terminal at random. The random number generation part 430 determines the session key (Session Key) at random furtherand the secret key treating part 460 enciphers by the public key of the receiving terminal Dand creates E_D [Session Key]. Since E_D [Session Key] can serve also as the meaning of Nonceit deletes Nonce in drawing 3 and transposes E_D [Session Key] to the position instead. The secret key treating part 460 obtains the output (pseudo-random number series) of a symmetrical key code using Session Key. The operation part 470 calculates the exclusive OR of transmit-terminal transient address ADD_Sreceiving terminal address ADD_Dcertificate $Cert_S$ of a transmit terminal and digital signature Sig_S (signature for all the field)and the above-mentioned pseudo-random number series. The transmission and reception section 426 sets the whole to RREQand carries out broadcast transmission.

[0046]
The relay terminal T1 which received RREQ assumes that RREQ which has specific length is RREQ from Sand does not perform verification of Sig_S (the management to this problem is mentioned later.)but carries out the same processing as drawing 3and is transmitted. A relay terminal also carries out same processing and is transmitted.
[0047]
The receiving terminal D which received RREQ from the relay terminal T2 performs the following processings.
[0048]
Encrypted common key E_D [Session Key] which received is decrypted using its own secret keyand a common key (Session Key) is obtained. The output (pseudo-random number series) of a symmetrical key code is obtained using Session Key obtained as a result of decoding. Data can be restored by taking the exclusive OR of the acquired pseudo-random number series and the field currently kept secret.
[0049]
In the case of a replyit re-enciphers using the newly created pseudo-random number series (it differs from the random number series at the time of reception) by the random number generation part of the receiving terminal D. That isthe exclusive OR of a new pseudo-random number seriesand $ADD_S$$ADD_D$$Cert_S$$Sig_S$ and SigD is taken. Thereforethe mask of the random number series of S and D will be given to ADD_S of RREP$ADD_D$$Cert_S$and Sig_Srespectively.
[0050]
S which received RREP transmitted via the relay terminal T1 and T2 performs the following processings.
[0051]
When verifying whether it is RREP addressed to itselfthe pseudo-random number series which the receiving terminal D set up is removed. Although reference was not made in particular about the use mode of the symmetrical key code until nowin order to output a pseudo-random number seriesuse with CTR mode is common.
[0052]
The outline in CTR mode is shown in drawing 9. As for Initialization Vector (henceforth the following)it is desirable that it is sharable in secrecy among transceiver persons. As for a counter (henceforth the following)in order to synchronize among transceiver persons and to reduce the influence of a step-outit is desirable to add a raw value to a packet and to transmit it.
[0053]
Drawing 10 is the example which assumed CTR mode in the use mode of the symmetrical key code in drawing 8. It explains below focusing on different processing from drawing 5.
[0054]
IV decides to connect with Session Key and to transmit (it displays with the sign of

"||" below)and is taken as Seed=Session Key || Iv. It enables it to choose ct independently with the transmit terminal S and the receiving terminal D (it is respectively considered as ct_S and ct_D)and it adds this field to the head of a packet. Since an order of a packet will leak to a third party if ct continues incrementallya sending person decides to assign a random value. Since ct also contained the implications of NonceED [Session Key] had been regarded as Nonce until nowbut belowct shall play the role of Nonce.

[Work example 3]

[0055]

Working example 3 of this invention is described referring to drawing 11 and 12. Although drawing 11 is the same figure as drawing 10it shows the information about the relay terminal (node) exposed by the third party by shading. If the necessity for relay information is considered anewin order for the transmit terminal S and the receiving terminal D to perform Source Routingit is necessary to get to know the information on all the relay terminal butand the relay terminal itself is enough if the following judgment can be performed.

[0056]

1. That check which is addressing to itself to RREQjustification of information from last relay terminal.

[0057]

2. Is he contained in a transmission address list to RREP or not?

[0058]

Thereforesince disclosure of unnecessary information has the danger of becoming an offensive materialit is desirable to conceal as much as possiblealso about the information on a relay terminalso that only the transmit terminal S and the receiving terminal D may be known. Sobelowthe example concealed so that only S and D may understand the shading field of drawing 11 for improvement in privacy is explained.

[0059]

In order to conceal the shading field of drawing 11drawing 12 applies a public key temporarily and shows at RREQ the example to which the object of the symmetrical key code was expanded by RREP. It explains below focusing on different processing from drawing 8 and drawing 10.

[0060]

The random number generation part 430 of the transmit terminal S determines the pair of a secret key (K−) at random in transmission of RREQ a public key (K+) and temporarily temporarily. Although secret key K− is added to RREQ public key K+ and temporarily temporarily and it transmitslet only secret key K− be an object of the exclusive OR of a pseudo−random number series temporarily.

[0061]

The relay terminal T2 which received RREQ carries out accumulation encryption of the information on a former relay terminal (in this case$ADD_{T1}Cert_{T1}Sig_{T1}$) using K+ from

itself. Even when the relay terminal which is malicious by carrying out accumulation encryption omits former relay terminal information by an inverse ramp from itselfit can avoid that detection becomes impossible with the receiving terminal D.

[0062]

The receiving terminal D which received RREQ performs the following processings.

[0063]

Sig for every relay path is verified. After verifying $Sig_{T2}ADD_{T2}Cert_{T2}$and Sig_{T2} are removed. The whole information on a relay terminal is decoded temporarily using secret key K−. Sig_{T1} is verified. $ADD_{T1}Cert_{T1}$and Sig_{T1} are removed. Sig_S is verified.

[0064]

Generallyonly the number of times of relay guessed from the length of the whole relay terminal information will repeat processing of a following series. That isthey are decodingverification of outermost Sigand processing of a series of removal of outermost additional information in secret key K− temporarily.

[0065]

When the receiving terminal D sends a replyto all the information copied from RREQexclusive OR with the pseudo−random number series (it differs from the random number series at the time of reception) newly created with the receiving terminal D is takenit re−enciphersand RREP is created. The object domain of a mask pattern will be expanded and a mask pattern will be applied also to K−K+E_D

[Seed]$ADD_{T1}Cert_{T1}Sig_{T1}ADD_{T2}Cert_{T2}$and Sig_{T2}.

[0066]

Since the mask pattern is hung on all the information copied from RREQADD_{T1} and ADD_{T2} are concealed and discernment of them becomes impossible in a relay terminal. Thenit stores in the relay address list field in which the raw value of ADD_{T1} and ADD_{T2} was established newly.

[0067]

The transmit terminal S which received the RREP signal performs the following processings.

[0068]

Encrypted common key E_D [Seed] which received is decrypted and verified. Since its address ADD_S cannot be discovered to a relay address lista random number series is removed. He recognizes that it is the response to RREQ which transmitted before from the combination of $ADD_SADD_DSeedCert_S$and Sig_S. Sig_D is verified. Sig for every relay path is verified. That isRREP is transposed to RREQ and Sig_D is removed. After verifying $Sig_{T2}ADD_{T2}Cert_{T2}$and Sig_{T2} are removed. After verifying $Sig_{T1}ADD_{T1}Cert_{T1}$and Sig_{T1} are removed. Relay path information (S−>T1−>T2−>D) is become final and conclusive.

[Work example 4]

[0069]

Working example 4 of this invention is described referring to drawing 13 and drawing

14. Although drawing 13 is the same figure as drawing 12it shows the information about the relay terminal (node) exposed by the third party by shading. It is desirable to conceal as much as possiblealso about the address of a relay terminalso that the transmit terminal Sthe receiving terminal Dand the relay terminal itself may be known. Thenworking example concealed so that the transmit terminal Sthe receiving terminal Dand the relay terminal itself may understand the shading field of drawing 13 for improvement in privacy is described.

[0070]

Although there is the method of making ADD_{T1} and ADD_{T2} a transient address as easy managementsince the relay address same for a while will be applied through two or more packetsthe danger of being exposed of the relevance of a packet exists only by this method. Thereforestructure stronger against disclosure of privacy is done by the direction where a different transient address for every packet is applied. In order to cope with this problempractical use of a public key and a hash function is considered temporarily.

[0071]

In order that drawing 14 may conceal the shading field of drawing 13in RREQit is the example which enciphered the random number by the public key temporarilyand applied the hash function to the random number in RREP. It explains below focusing on different processing from drawing 9. The random number which $rand_X$ determined at the terminal Xand h (y) mean the hash value of y. A hash function means the existing function and procedure for summarizing from enumeration of character stringssuch as a document and a numberto fixed length's data. The value outputted through a function is called a "hash value." The hash function "SHA-1" and "MD5" is typicaland since all are one directional functionsit is impossible to presume the original text from generated data. If both are compared in quest of the hash value of data at the both ends of a course when transmitting and receiving data through a communication lineit can be investigated whether data is altered in the middle of communication.

[0072]

The relay terminal T1 which received RREQ sets up E_{K+} [$rand_{T1}$] instead of address ADD_{T1} of self.

[0073]

T2 performs the same processing as T1.

[0074]

D which received RREQ acquires $rand_{T1}$ and $rand_{T2}$ and applies h ($rand_{T1}||ct_D$) and h ($rand_{T2}||ct_D$) instead of ADD_{T1} and the raw value of ADD_{T2}.

[0075]

T2 which received RREP recognizes its address as h ($rand_{T2}||ct_D$).

[0076]

T1 performs the same processing as T2.

[0077]
The transmit terminal S which received RREP performs the following processings.
[0078]
h ($rand_S||ct_D$) is inspected when discovering its address with a relay address list. $rand_{T1}$ and $rand_{T2}$ are acquired.
[Work example 5]
[0079]
Working example 5 of this invention is described referring to drawing 14 thru/or drawing 16.
[0080]
When drawing 14 is referred tothe packet length of RREQ and the relay address list of RREP show that the danger that the information about the transmit terminal S and the receiving terminal D will leak as follows is high.
[0081]
- RREQ : packet length shows that the relay terminal T1 is next to the receiving terminal S.
[0082]
- RREP : if the relay terminal T1 and the relay terminal T2 conspire (conspiracy)a relay address list shows that the receiving terminal D is a next door (next door of ST1) of the relay terminal T2. Thenthe example which utilizes dummy information (random number) and conceals the information on the transmit terminal S and the receiving terminal D as much as possible to the transmit terminal S and the receiving terminal D by [which is a relay terminal / that] making it act like is explained.
[0083]
Drawing 15 gives each of the RREQ signal from the transmit terminal Sand the RREP signal from the receiving terminal D dummy informationand it is made to serve it as if both terminals were relay terminals. It explains below focusing on different processing from the above-mentioned example. The transmit terminal S gives dummy relay terminal information (Dummy1Dummy2 which mean a part for 1 relay by drawing 15) into a RREQ signal. Since dummy information existseven if exposed of the information on the transmit terminal Sit sees from a third party and distinction with a master station and a relay terminal does not stick.
[0084]
The relay terminal T1 which received the RREQ signal verifies Sig_S. Since verification of Sig_S was not completed in the example of the just before aboveit assumed that RREQ of specific length was RREQ from Sand verification of Sig_S was not performed. In this examplesince S carried out **** of a relay terminalcertificate $Cert_S$ could be revealedand attestation became possible.
[0085]
D which received RREQ performs the following processings.
[0086]

It decrypts temporarily using secret key K-and Sig for every relay path is verified in an order from the re-outsideand verification processing is repeated until $Cert_S$ appears. Although only the number of times of relay guessed from the length of the whole relay node information had repeated processing in the example of the just before abovesince S carries out **** of a relay terminalthe method is inapplicable by this example.

[0087]

In the receiving terminal Da dummy address (drawing 15 DummyADD1 for twoDummyADD2) is added to the relay address list of a RREP signaland exclusive OR with a pseudo-random number series is taken.

[0088]

The transmit terminal S which received the RREP signal verifies Sig for every relay path like the transmit terminal D.

[0089]

Herewhen drawing 15 is seen wellit turns out that there is a danger that the information about the number of relay stages will leakfrom the packet length of a RREP signal. First of allthe contents of the RREP signal are enough if the transmit terminal S and the receiving terminal D can be recognizedand a third party does not need to identify. Thenthe example which conceals the history of a RREP signal as much as possible is explained below.

[0090]

Drawing 16 is the example which concealed the history of RREP as much as possible. It explains below focusing on different processing from the above-mentioned example.

[0091]

The receiving terminal D performs the following processings in creation of a RREP signal.

[0092]

Instead of RREPthe transmit terminal S adds the 2nd identification field (RREP/Data) that can distinguish RREP or Data. Padding of dummy information (random number) is added (Dummy Padding in drawing 16). The Length field is added and the length except Dummy Padding is set up. The mask pattern which the receiving terminal D set up is covered over threethe 2nd identification fieldDummy Paddingand Length.

[0093]

The transmit terminal S which received RREP/Data performs the following processingsafter removing the mask pattern which the receiving terminal D set up.

[0094]

1. Recognize that it is RREP from the 2nd identification field.

[0095]

2. Remove Dummy Padding in consideration of the Length field.

[Work example 6]

[0096]

Working example 6 of this invention is shown in drawing 17. Working example 6 shown in drawing 17 is an example of the mode included all above-mentioned working example. Thereforeexplanation is omitted.

[Work example 7]

[0097]

Nexttemporarilysupposing T2 is a malicious relay terminalthe relay terminal T2 can cancel the information on the relay terminal T1 intentionally. Thenthe example for coping with such an evil deed is explained below.

[0098]

It explains with reference to drawing 17. The mechanism of detecting the information on the relay terminal T1 having been canceled by giving indivisible relation to the information on the relay terminal T1 and the information on terminal Dummy2 in front of that is considered.

[0099]

As shown in drawing 18in the relay terminal T1encryption by the block cipher which uses K_{T1}= h ($rand_{T1}Cert_{T1}$) based on the information on the relay terminal T1 as a key is given to the information on Dummy2 which is a terminal in front of that. $rand_{T1}$ is a certificate of the terminal T1 in which a certificate issue section publishes the random number determined at the terminal T1and $Cert_{T1}$.

h (y) means the hash value of y.

[0100]

Also in the relay terminal T2encryption by the block cipher which uses K_{T2}= h ($rand_{T2}Cert_{T2}$) based on the information on the relay terminal T2 as a key is given to the information on T1 which is a terminal in front of that. Thereforein order to restore this encryptionthe receiving terminal D needs to get to know right relay terminal information.

[0101]

Although this example was described taking the case of the case where Dummy is usedthe invention concerning this example can be applied also about the relay terminal which existsand can be applied also to the other various composition. The arbitrary terminal information of not only the last terminal information but the upper stream may be enciphered.

[0102]

Even if a malicious relay terminal cancels the information on an upstream relay terminal intentionally by having the above compositionin the receiving terminal Dthe information on the terminal in front of the canceled relay terminal will be decoded correctly. In this waythe receiving terminal D can detect this forged course.

[0103]

Thusaccording to this examplewithout enlarging the processing load by a relay terminal so muchforgery of the relay terminal information by a malicious relay terminal

can be preventedchannel information can be concealed so that it cannot forgeand a transceiver person's privacy to a third party improves.

[Industrial applicability]

[0104]

In the radio or the wire communication field as which secrecy is requiredthe communication terminal and ad hoc network path control method according to this invention can be used.

[Brief Description of the Drawings]

[0105]

[Drawing 1]It is a key map showing the outline of the conventional ad hoc network.

[Drawing 2]It is a schematic block diagram of the moving terminal in which the conventional ad hoc network construction is possible.

[Drawing 3]It is a chart which shows the data of the path control signal for the conventional ad hoc network construction.

[Drawing 4]It is a block diagram of the moving terminal according to working example of this invention.

[Drawing 5]It is a chart according to working example 1 which shows the data of the path control signal for ad hoc network construction.

[Drawing 6]It is a chart which shows the data of the path control signal for describing working example 2and disclosure of the sender receiver terminal to a third party is shown.

[Drawing 7]It is a chart according to working example 2 which shows the data of the path control signal for ad hoc network constructionand the transient address is used for ADDS.

[Drawing 8]It is a chart according to working example 2 which shows the data of the path control signal for ad hoc network constructionand the hybrid code is used.

[Drawing 9]It is a key map according to working example 2 showing the outline in CTR mode.

[Drawing 10]It is a chart according to working example 2 which shows the data of the path control signal for ad hoc network constructionand CTR mode is used.

[Drawing 11]It is a chart which shows the data of the path control signal for describing working example 3and disclosure of the relay information to a third party is shown.

[Drawing 12]It is a chart according to working example 3 which shows the data of the path control signal for ad hoc network constructionand the public key is used temporarily.

[Drawing 13]It is a chart which shows the data of the path control signal for describing working example 4and disclosure of the relay terminal address to a third party is shown.

[Drawing 14]It is a chart according to working example 4 which shows the data of the path control signal for ad hoc network constructionand use of the hash function is

shown.
[Drawing 15]It is a chart according to working example 5 which shows the data of the path control signal for ad hoc network constructionand dummy information is added.
[Drawing 16]It is a chart according to working example 5 which shows the data of the path control signal for ad hoc network constructionand is the example which concealed the history of RREP as much as possible.
[Drawing 17]It is the chart which each working example contained altogether and which shows the data of the path control signal for ad hoc network construction.
[Drawing 18]It is a chart according to working example 7 which shows the data of the path control signal for ad hoc network constructionand is an example which prevents cancellation of a relay terminal.
[Description of Notations]
[0106]
400 Moving terminal
422 Request/reply generating part
424 Control section
426 Transmission and reception section
427 Address storage section
428 Address comparison part
430 Random number generation part
440 Certificate issue section
450 Digital signature preparing part
460 Secret key treating part
470 Operation part
480 Verification part

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[0105]
[Drawing 1]It is a key map showing the outline of the conventional ad hoc network.
[Drawing 2]It is a schematic block diagram of the moving terminal in which the conventional ad hoc network construction is possible.
[Drawing 3]It is a chart which shows the data of the path control signal for the conventional ad hoc network construction.
[Drawing 4]It is a block diagram of the moving terminal according to working example of this invention.
[Drawing 5]It is a chart according to working example 1 which shows the data of the path control signal for ad hoc network construction.
[Drawing 6]It is a chart which shows the data of the path control signal for describing

working example 2and disclosure of the sender receiver terminal to a third party is shown.

[Drawing 7]It is a chart according to working example 2 which shows the data of the path control signal for ad hoc network constructionand the transient address is used for ADDS.

[Drawing 8]It is a chart according to working example 2 which shows the data of the path control signal for ad hoc network constructionand the hybrid code is used.

[Drawing 9]It is a key map according to working example 2 showing the outline in CTR mode.

[Drawing 10]It is a chart according to working example 2 which shows the data of the path control signal for ad hoc network constructionand CTR mode is used.

[Drawing 11]It is a chart which shows the data of the path control signal for describing working example 3and disclosure of the relay information to a third party is shown.

[Drawing 12]It is a chart according to working example 3 which shows the data of the path control signal for ad hoc network constructionand the public key is used temporarily.

[Drawing 13]It is a chart which shows the data of the path control signal for describing working example 4and disclosure of the relay terminal address to a third party is shown.

[Drawing 14]It is a chart according to working example 4 which shows the data of the path control signal for ad hoc network constructionand use of the hash function is shown.

[Drawing 15]It is a chart according to working example 5 which shows the data of the path control signal for ad hoc network constructionand dummy information is added.

[Drawing 16]It is a chart according to working example 5 which shows the data of the path control signal for ad hoc network constructionand is the example which concealed the history of RREP as much as possible.

[Drawing 17]It is the chart which each working example contained altogether and which shows the data of the path control signal for ad hoc network construction.

[Drawing 18]It is a chart according to working example 7 which shows the data of the path control signal for ad hoc network constructionand is an example which prevents cancellation of a relay terminal.

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-286989
(P2005-286989A)
(43)公開日　平成17年10月13日(2005.10.13)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/28	H04L 12/28	307	5K030
H04L 12/56	H04L 12/56	100D	5K033

審査請求 未請求　請求項の数 11　OL　（全 20 頁）

(21)出願番号　特願2004-250816 (P2004-250816)
(22)出願日　平成16年8月30日 (2004.8.30)
(31)優先権主張番号　特願2004-58072 (P2004-58072)
(32)優先日　平成16年3月2日 (2004.3.2)
(33)優先権主張国　日本国(JP)

(71)出願人　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　萩原　淳一郎
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　青木　秀憲
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　梅田　成視
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内

Fターム(参考)　5K030 GA15　JL01　LB05

最終頁に続く

(54)【発明の名称】通信端末及びアドホックネットワーク経路制御方法

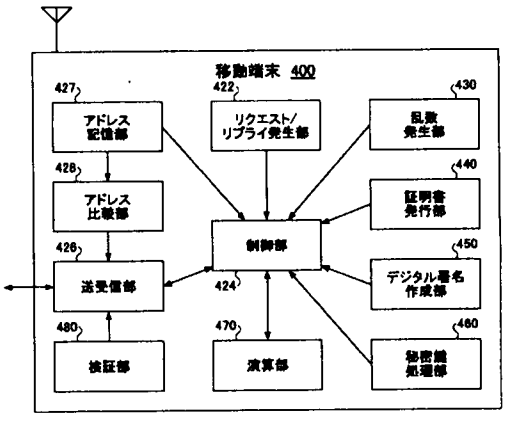
(57)【要約】

【課題】　アドホックネットワークにおいて、誤った経路制御情報を信じてしまう危険性を回避し、送受信端末や中継端末のアドレス情報等を可能な限り隠蔽する経路制御方法等を提供すること。

【解決手段】　アドホックネットワーク経路の生成が可能な通信端末が、他の通信端末との通信を行う送受信部；アドホックネットワーク経路の生成を要求する経路要求メッセージを発生する経路要求発生部；自己端末のアドレスと受信端末のアドレスを記憶するアドレス記憶部；乱数を発生する乱数発生部；自己端末の証明書を発行する証明書発行部；自己端末のデジタル署名を作成するデジタル署名作成部；アドホックネットワークプロトコルに従って、自己端末のアドレス、受信端末のアドレス、乱数、証明書及びデジタル署名を経路要求メッセージに付加して構成したデータを、送受信部を介して送受信する制御部；から構成される。

【選択図】　図4

本発明の実施例に従った移動端末のブロック図



【特許請求の範囲】
【請求項１】
アドホックネットワーク経路の生成が可能であり、他の通信端末との通信を行う送受信部とアドホックネットワーク経路の生成を要求する経路要求メッセージを発生する経路要求発生部とを有する通信端末であって：
自己端末のアドレスと受信端末のアドレスを記憶するアドレス記憶部；
乱数を発生する乱数発生部；
自己端末の証明書を発行する証明書発行部；
自己端末のデジタル署名を作成するデジタル署名作成部；
アドホックネットワークプロトコルに従って、自己端末のアドレス、受信端末のアドレス、前記の乱数、証明書及びデジタル署名を前記経路要求メッセージに付加して構成したデータを、前記送受信部を介して送受信する制御部；
から構成される通信端末。
【請求項２】
請求項１記載の通信端末であってさらに：
秘密鍵を作成して、前記データの少なくとも一部を暗号化する秘密鍵処理部；及び
受信した被暗号化データを復号する演算部；
から構成される通信端末。
【請求項３】
複数の通信端末間にアドホックネットワークを生成するためのアドホック経路制御方法であって：
送信端末において、アドホック経路要求信号に送信端末アドレス、受信端末アドレス及び送信端末デジタル署名を付加して構成したデータをブロードキャスト送信する段階；
中継端末において、送信端末から送信された送信端末デジタル署名を認証し、前記アドホック経路要求信号に中継端末アドレス及び中継端末デジタル署名を付加してブロードキャスト転送する段階；
受信端末において、前記中継端末デジタル署名及び前記送信端末デジタル署名を認証する段階；及び
前記受信端末において、受信した前記データに受信端末デジタル署名を付加して構成したアドホック経路応答信号を前記送信端末に宛てて送信する段階；
から構成されるアドホック経路制御方法。
【請求項４】
複数の通信端末間にアドホックネットワークを生成するためのアドホック経路制御方法であって：
送信端末において、アドホック経路要求信号に送信端末アドレス及び受信端末アドレスを付加して構成したデータの少なくとも一部に受信端末の公開鍵を用いて暗号化を行い、前記データをブロードキャスト送信する段階；
中継端末において、前記アドホック経路要求信号に中継端末アドレスを付加してブロードキャスト転送する段階；
受信端末において、受信した前記データを付加したアドホック経路応答信号を前記送信端末に宛てて送信する段階；
から構成されるアドホック経路制御方法。
【請求項５】
請求項３に記載のアドホック経路制御方法であって、前記の受信端末における認証段階において、前記受信端末が、受信した前記データを自己の秘密鍵を用いて復号化する段階をさらに有することを特徴とするアドホック経路制御方法。
【請求項６】
請求項４に記載のアドホック経路制御方法であって、前記の送信端末における暗号化段階において、前記送信端末がセッションキーを決定し、そのセッションキーを用いたハイブリッド暗号化を行う段階を有する、ことを特徴とするアドホック経路制御方法。

【請求項７】
上記請求項の何れかに記載のアドホック経路制御方法であって、前記の中継端末アドレスを隠蔽する段階をさらに有することを特徴とするアドホック経路制御方法。
【請求項８】
請求項７に記載のアドホック経路制御方法であって、前記の中継端末アドレスを隠蔽する段階が、中継端末の情報の一部を利用して上流の中継端末の情報を隠蔽する段階から成ることを特徴とするアドホック経路制御方法。
【請求項９】
上記請求項の何れかに記載のアドホック経路制御方法であって、前記データ中にダミーアドレスを挿入する段階をさらに有することを特徴とするアドホック経路制御方法。
【請求項１０】
上記請求項の何れかに記載のアドホック経路制御方法であって、前記データ中にダミーパディングを挿入する段階をさらに有することを特徴とするアドホック経路制御方法。
【請求項１１】
請求項１又は２に記載の通信端末を送信端末として含み、さらに、中継端末及び受信端末を含むアドホックネットワークシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、アドホックネットワーク経路制御方法及びそのための通信端末に関し、特に認証やプライバシー保護のための処理を行うアドホックネットワーク経路制御方法及びそのための通信端末に関する。
【背景技術】
【０００２】
移動通信需要の急拡大・多様性に伴い、移動通信基地局がカバーする領域の外部にある移動通信端末から移動通信網へ接続することの需要がある。移動通信基地局のカバー領域外にある移動通信端末から基地局への直接的なワンホップ接続が不可能であることから、他の移動通信端末や一時的に設置した簡易中継局を介して基地局にマルチホップ接続するワイヤレスアドホックネットワークを利用する方法が提案されている。すなわち、ワイヤレスアドホックネットワークとは、ユーザの利用する携帯端末や一時的に設置した簡易中継局等によって一時的に構築される無線ネットワークである（図１参照）。各移動通信端末および簡易中継局は、アドホックルーティングプロトコルを内蔵し、これに従って各端末間で自発的な情報の送受信を行い、アドホックネットワークを構成する。アドホックネットワークでは、種々の端末に情報が受信されてしまうことから、セキュリティ、プライバシーを確保することが重要である。
【０００３】
アドホックネットワークの一例として、端末からの経路設定要求が生じた際に経路を生成するDSR(Dynamic Source Routing)方式がある。DSR方式では、送信端末が、受信端末までの経路上の全端末（ノード）のアドレスを知ることにより、その経路を使ってデータを送ることができる。データを中継する端末（ノード）は、転送される経路情報を利用して次の転送先を知ることができるため、中継端末が経路情報を持つ必要がなく、比較的軽い処理で済む。アドホックネットワークを利用することにより、移動通信網の提供する通信エリアの外にある移動通信端末に対しても、セルラー通信サービスやインターネット接続サービス等を提供することが可能となる。このような通信形態において、アドホックネットワークと移動通信網の双方の構成要素として稼働し、アドホックネットワークから移動通信網への通信路の橋渡しを担う通信端末を、関門端末と呼ぶ（図１の１６参照）。ここで、関門端末Ｄは、移動通信網に直接接続している通信端末の別称であるから、任意の通信端末が関門端末Ｄとなることができる。また、関門端末Ｄが移動通信網の提供するエリアの外へと移動した場合、もはや関門端末にはなれず、単なる移動通信端末となる。
【０００４】

アドホックネットワークは、例えば図１に示すように構成される。移動無線通信の例で説明するが、アドホックネットワークは、無線に限られず有線通信においても有用である。移動端末Ｓ（１２）は、アドホック経路制御プロトコルに従って、アドホックネットワークを形成する。図示の例では、移動通信端末Ｓ（１２）が中継端末Ｔ１（１４）及び中継端末Ｔ２（１５）を経由して関門端末Ｄ（１６）に接続されて、アドホックネットワークを構成している。関門端末Ｄ（１６）が基地局Ｂ（１８）のカバーするエリア内にいるので、移動端末Ｓ（１２）は関門端末Ｄ（１６）を経由して基地局Ｂ（１８）に接続してそこからのサービスを受けることができる（特許文献１参照）。

【０００５】

ここで、IETF（The Internet Engineering Task Force，インターネットのよりよいアーキテクチャやスムーズなオペレーションを目的に、インターネットの標準化を中心にボランティア活動を展開している団体）のMANET（Mobile Ad-hoc Networks） WG（作業部会）で検討されているDSR（Dynamic Source Routing）における経路制御の従来例の概要を図２及び図３に示す。

【０００６】

図２及び図３を参照しながら、従来の経路確立の手順を説明する。図２及び図３に示す送信端末Ｓ（Source）は、図１の移動端末Ｓに相当するものとして説明するが、これに限られず、関門端末でも良いし、他の移動端末であっても良い。図２及び図３に示す受信端末Ｄ（Destination）は、図１の関門端末Ｄに相当するものとして説明するが、これに限られず、移動端末であっても良い。図２及び図３に示す中継端末Ｔ（Transmitter）、Ｔ１，Ｔ２は、図１の中継端末１４，１５に相当するものとして説明するが、これに限られない。図３の中継端末Ｔ１、Ｔ２は構成及び機能が同じであるので、図２においては１つの中継端末Ｔが代表して示されている。

【０００７】

送信端末Sが受信端末Dとの通信を開始する際、リクエスト／リプライ発生部２２２が、アドホックネットワーク経路の生成を要求するための制御メッセージであるRREQ（Route REQuest）という信号を発生させ、送受信部２２６がRREQをネットワークへブロードキャスト送信する。送信端末のアドレスADD_Sと受信端末のアドレスADD_Dがアドレス記憶部２２７から読み出され、RREQに付加され、一緒に送信される。アドレスは、例えばIPアドレスであってよい。制御メッセージPREQには、再転送するホップ数を制限する情報を含んでも良い。

【０００８】

制御メッセージRREQを送受信部２４６によって受信した中継端末T1は、アドレス記憶部２４７内に記憶された自分のアドレスADD_{T1}と受信したアドレスADD_Dとを比較して、自分宛で無いことが分かると、自分のアドレスADD_{T1}を付加して、RREQをブロードキャストで転送する。

【０００９】

中継端末Ｔ２も端末Ｔ１と同様の転送処理を行う。

【００１０】

制御メッセージRREQを受信した受信端末Dは、アドレス記憶部２６７内に記憶された自分のアドレスとADD_Dを比較して自分宛であることが分かると、RREP（Route REPly）という制御メッセージに中継アドレス情報をコピーしたものを付加して、ユニキャストで送信端末Ｓへと返信する。

【００１１】

RREPを受信した中継端末Ｔ２は、中継アドレスリストに自分のアドレスを発見すると、この信号をユニキャストで転送する。

【００１２】

中継端末Ｔ１も端末Ｔ２と同様の処理を行う。

【００１３】

RREPを受信した送信端末Ｓは、アドレス情報ADD_SとADD_Dの組み合わせから、この信号は

自分が以前に送信したRREQに対する応答であることを認識でき、中継経路情報（Ｓ→Ｔ１→Ｔ２→Ｄ）を知ることができる。

【特許文献１】特開２００３－２３０１６７号公報

【発明の開示】

【発明が解決しようとする課題】

【００１４】

しかしながら、従来技術におけるDSRアドホックネットワークでは、経路制御信号であるRREQやRREPの認証を行っていないため、誤った経路制御情報を信じてしまう危険性があった。また、送受信者情報や中継ノードのアドレス情報等を誰でも読める状態でヘッダに格納するため、第三者が送受信者を特定する事が可能であり、プライバシー上の問題等があった。

【００１５】

そこで、本発明の課題は、アドホックネットワークにおいてRREQとRREPの認証を行うことにより、誤った経路制御情報を信じてしまう危険性を回避できるような経路制御方法等を提供することである。

【００１６】

また、送受信端末や中継端末のアドレス情報等を可能な限り隠蔽することにより、第三者に対する送受信端末のプライバシーを向上できるような経路制御方法等を提供することである。

【課題を解決するための手段】

【００１７】

上記の課題を達成するための本発明の一特徴に従った、アドホックネットワーク経路の生成が可能であり、他の通信端末との通信を行う送受信部とアドホックネットワーク経路の生成を要求する経路要求メッセージを発生する経路要求発生部とを有する通信端末は、自己端末のアドレスと受信端末のアドレスを記憶するアドレス記憶部；乱数を発生する乱数発生部；自己端末の証明書を発行する証明書発行部；自己端末のデジタル署名を作成するデジタル署名作成部；アドホックネットワークプロトコルに従って、自己端末のアドレス、受信端末のアドレス、乱数、証明書及びデジタル署名を経路要求メッセージに付加して構成したデータを、送受信部を介して送受信する制御部；から構成される。

【００１８】

このような移動通信端末はさらに、秘密鍵を作成して、データの少なくとも一部を暗号化する秘密鍵処理部；及び受信した被暗号化データを復号する演算部を有しても良い。

【００１９】

上記の課題を達成するための本発明の一特徴に従った、複数の通信端末間にアドホックネットワークを生成するためのアドホック経路制御方法は、送信端末において、アドホック経路要求信号に送信端末アドレス、受信端末アドレス及び送信端末デジタル署名を付加して構成したデータをブロードキャスト送信する段階；中継端末において、送信端末から送信された送信端末デジタル署名を認証し、アドホック経路要求信号に中継端末アドレス及び中継端末デジタル署名を付加してブロードキャスト転送する段階；受信端末において、中継端末デジタル署名及び送信端末デジタル署名を認証する段階；及び受信端末において、受信したデータに受信端末デジタル署名を付加して構成したアドホック経路応答信号を送信端末に宛てて送信する段階；から構成される。

【発明の効果】

【００２０】

本発明の実施例に従えば、RREQとRREPの認証を行うことで、誤った経路制御情報を信じてしまう危険性を回避することができる。また、送受信端末や中継端末のアドレス情報等を可能な限り隠蔽することにより、第三者に対する送受信端末のプライバシー保護を向上させることができる。

【発明を実施するための最良の形態】

【００２１】

以下、図面を参照しながら本発明の各実施例について説明する。先ず、本発明の各実施例についての前提を述べる。

【００２２】

・何らかの手段によって、全ノード（端末）がルートCA（Certificate Authority，認証局）の証明書を保持しており、自分の証明書を発行でき、秘密鍵を作成可能である。

【００２３】

・何らかの手段によって、通信開始前に通信相手のアドレスと証明書を知ることができる。

【実施例１】

【００２４】

図４及び図５を参照しながら、本発明の実施例１を説明する。本発明の実施例に従った移動端末４００は、リクエスト／リプライ発生部４２２，制御部４２４，送受信部４２６，アドレス記憶部４２７，アドレス比較部４２８，乱数発生部４３０，証明書発行部４４０，デジタル署名作成部４５０，秘密鍵処理部４６０、演算部４７０及び検証部４８０を有している。この構成は、送信端末に限られず、中継端末や受信端末も同様な構成を有する。本発明は、移動無線通信に限られず、有線通信に対しても適用可能である。

【００２５】

リクエスト／リプライ発生部４２２で発生された経路要求制御メッセージRREQを、送受信部４２６がネットワークへブロードキャスト送信する。

【００２６】

実施例１においては、図５に示されているように、RREQでは、各ホップ間（すなわち、送信端末Ｓ→中継端末Ｔ１→中継端末Ｔ２→受信端末Ｄの間）に認証を適用し、RREPでは、エンド間（すなわち、受信端末Ｄ→送信端末Ｓの間）のみに認証を適用している。図５のうち図３と異なる部分は、網掛けして示している。図５に示すNonceは、乱数発生部４３０にて発生された乱数を意味する。$Cert_X$は、証明書発行部が発行する端末Xの証明書を意味する。Sig_Xは、端末Xによるデジタル署名であり、デジタル署名作成部により作成される。

【００２７】

従来例のDSRにおいては、RREQ，RREPの認証を行っていないが、本実施例においては、これらの信号の認証を行うものである。RREQで中継ノード毎の認証を行うので、返信のRREPではエンド間の認証で十分であると考えられる。

【００２８】

以下に各端末の動作につき説明する。先ず送信端末Ｓの乱数発生部４３０が、乱数Nonceを決定する。証明書発行部４４０が、$Cert_S$を発行する。制御部４２４が、制御メッセージRREQにNonceと自身の証明書$Cert_S$を付加する。乱数Nonceを付加するのは、ネットワークを再送攻撃から守るためである。また、受信端末は送信端末の情報を必ずしも知るわけではないため、RREQに送信端末自身の証明書を付加しておく。Nonceと証明書$Cert_S$を付加した信号RREQの全フィールドを対象として、デジタル署名作成部４５０が、自身のデジタル署名Sig_Sを作成する。Nonce，$Cert_S$及びSig_Sが付加された信号RREQを、送受信部４２６がブロードキャストでネットワークに送信する。

【００２９】

信号RREQを受信した中継端末Ｔ１の検証部４８０が、公知の方法で、受信した信号RREQに含まれるNonceの検証を行う。もし、Nonceが、以前受信したNonceの値と同じ場合には、今回のRREQが再送信であると認識して破棄する。Nonceが初めて受信する値である場合には、検証部４８０が、付加されている証明書$Cert_S$を用いて、送信端末のデジタル署名Sig_Sを公知の方法で検証する。検証の結果、問題が無ければ、ADD_Dと自分のアドレスとを比較して自分宛で無いことを確認する。次に、受信した信号に中継端末Ｔ１自身のアドレスADD_{T1}と証明書$Cert_{T1}$とを付加し、付加した信号全体に対して中継端末Ｔ１自身のデジタル署名Sig_{T1}を作成する。ADD_{T1}，$Cert_{T1}$，Sig_{T1}を付加したRREQをネットワークへブロードキャストで転送する。

【００３０】
中継端末Ｔ２も中継端末Ｔ１と同様の処理を行う。ただし、付加されている証明書$Cert_{T1}$を用いて、中継端末Ｔ１のデジタル署名Sig_{T1}を検証し、中継端末Ｔ１から受信したRREQ信号にADD_{T2}，$Cert_{T2}$，Sig_{T2}を付加してネットワークへブロードキャストで転送する。
【００３１】
中継端末Ｔ２からのRREQ信号を受信した受信端末Dの検証部４８０は、Nonceの検証を行う。もし、Nonceが、以前受信したNonceの値と同じ場合には、今回のRREQが再送信であると認識して破棄する。Nonceが初めて受信する値である場合には、付加されている証明書$Cert_{T2}$を用いて、中継端末のデジタル署名Sig_{T2}を検証する。ADD_Dと自分のアドレスとを比較して自分宛であることを認識する。付加されている証明書$Cert_{T1}$を用いて、中継端末のデジタル署名Sig_{T1}を検証する。付加されている証明書$Cert_S$を用いて、送信端末のデジタル署名Sig_Sを検証する。これらの処理の順番は、変更しても良い。
【００３２】
受信端末Ｄのリクエスト／リプライ発生部により発生した応答制御メッセージRREPに対して、RREQの内容のコピーを付加する。RREQの内容のコピーを付加したRREP信号の全フィールドを対象として、受信端末Ｄのデジタル署名Sig_Dを作成する。Sig_Dを付加したRREPをユニキャストで送信端末Ｓ宛に送信する。
【００３３】
受信端末ＤからのRREP信号を受信した中継端末Ｔ２は、Nonceの検証を行う。中継アドレスリストに自分のアドレスADD_{T2}を発見できるため、この信号をそのままユニキャストで転送する。
【００３４】
中継端末Ｔ１も中継端末Ｔ２と同様の処理を行う。
【００３５】
中継端末Ｔ１経由でRREP信号を受信した送信端末Ｓの検証部４８０は、先ずNonceの検証を行った後、以下の処理を行う。中継アドレスリストに自分のアドレスADD_Sを発見できないため、自分宛のRREPであるかどうかを検証する。ADD_S，ADD_D，Nonce、$Cert_S$，Sig_Sの組み合わせから、自分が以前に送信したRREQに対する応答であることを認識する。Sig_Dを検証する。中継経路毎のSigを検証する。すなわち、RREPをRREQに置きかえてSig_Dを除去する。Sig_{T2}を検証した後、ADD_{T2}，$Cert_{T2}$，Sig_{T2}を除去する。Sig_{T1}を検証した後、ADD_{T1}，$Cert_{T1}$，Sig_{T1}を除去する。中継経路情報（S→Ｔ１→Ｔ２→D）を確定する。
【実施例２】
【００３６】
図６乃至図１０を参照しながら、本発明の実施例２について説明する。図６は、図５と同様な図であるが、第三者に露呈されるＳとＤに関する情報を網掛けで示している。図６に示されるように、実施例１においては、プライバシーを保護できないという問題点がある。例えば、利用ユーザが限定される地域では、証明書の総当たりで、$Cert_S$が、ひいては送信端末Ｓが判明してしまう危険性がある。
【００３７】
そこで、プライバシー保護向上のために、図６の網掛けフィールドをSとDにしか分からないように暗号化して隠蔽する実施例を説明する。基本的な暗号方式である共通鍵暗号方式は、送信端末Ｓが平文データを共通鍵を用いて暗号化し、暗号化したデータを送信し、それを受信した受信端末Ｄが同じ共通鍵を用いて復号化する方式である。暗号化と復号化が逆方向の同じ処理であるところから、「対称アルゴリズム」とも呼ばれる。暗号化と復号化に同じ鍵を使うことから、高速な処理が可能となる。しかし、第三者に「共通鍵」が漏れてしまうと、その後の暗号を全て解読されてしまう危険性が高くなるという不利点がある。
【００３８】
図７に示す例では、送信端末ＳのアドレスADD_Sとして一時アドレスを適用し、その他には公開鍵暗号化を純粋に適用した方法を説明する。公開鍵暗号方式又は非対称アルゴリズ

ムとは、暗号化に使用する鍵と復号化に使用する鍵として、それぞれ違う鍵を用いる方式である。相手に公開した片方の鍵を「公開鍵」と呼ぶ。受信端末が「秘密鍵」と「公開鍵」をペアで作成する。「公開鍵」の方は公開し、「秘密鍵」は受信端末で保管しておく。送信端末は、受信端末の公開鍵を入手し、その鍵を用いて平文データの暗号化を行い、被暗号化データを送信する。被暗号化データを受信した受信端末は、保管しておいた秘密鍵を用いて被暗号化データを復号化する。

【００３９】

ここで、E_X［y］とはXの公開鍵を用いて平文yを暗号化することを意味している。図７に示す送信端末Ｓにおいて、受信端末ＤのアドレスADD_D、送信端末Ｓの証明書$Cert_S$及びデジタル署名Sig_Sを、受信端末Dの公開鍵で暗号化（E_D［ADD_D］，E_D［$Cert_S$］，E_D［Sig_S］）する。これらの被暗号化データを受信した受信端末Ｄは、保管しておいた秘密鍵を用いて復号化する。返信する際には、自己のデジタル署名Sig_Dを、送信端末Ｓの公開鍵で暗号化（E_S［Sig_D］）する。しかし、この方法には以下の問題がある。

【００４０】

１．公開鍵暗号のアルゴリズムによっては（オリジナルのRSA等）、同じ平文に対する暗号結果は常に同じ値になるため、ADD_Dは不明だがE_D［ADD_D］という“新しい”アドレスが常に露呈され、追跡される危険性が存在する。

【００４１】

２．一時アドレスに対しても、同じような危険性が存在する。

【００４２】

従って、同じ値を暗号化するとしても、毎回異なる結果が得られるようにした方が、よりプライバシーの漏洩に対する強い対策ができあがる。

【００４３】

この問題に対する実施例として、図８に示すようなハイブリッド暗号を適用した実施例２を説明する。ハイブリッド暗号方式によれば、送受信端末で以下のような処理を行う。予め、送受信端末Ｓ，Ｄ双方が共通鍵を共有している。受信端末Ｄが「秘密鍵」と「公開鍵」をペアで作成する。「公開鍵」の方は公開し、「秘密鍵」は受信端末Ｄで保管しておく。送信端末Ｓは、受信端末Ｄの公開鍵を入手し、その公開鍵を用いて共通鍵を暗号化して受信端末Ｄに送る。送信端末Ｓが、暗号化した共通鍵を用いて、平文データの対称鍵暗号化を行い、被暗号化データを送信する。公開鍵で暗号化された共通鍵と被暗号化データとを受信した受信端末Ｄは、保管しておいた秘密鍵を用いて被暗号化共通鍵を復号化する。その復号化された共通鍵を用いて、被暗号化データを復元する。平文データ自体は、速度の速い共通暗号化方式で暗号化／復号化を行うため、高速の処理速度が得られる。秘密性を高めるために、上記の共通鍵をセッション毎に変更することも可能である。その場合には、送信端末Ｓが、セッション毎に使い捨ての共通鍵（Session Keyと呼ぶ）を用いてデータの対称鍵暗号化を行い、Session Keyを公開鍵で暗号化して受信端末Ｄに通知する。

【００４４】

図８に示す実施例においては、送信端末アドレスADD_Sには一時アドレスを適用し、その他にはハイブリッド暗号を適用する。以下に、図３とは異なる処理を中心に説明する。

【００４５】

送信端末Ｓの乱数発生部４３０（図４参照）が、送信端末の一時アドレスADD_Sをランダムに決定する。乱数発生部４３０がさらにセッションキー（Session Key）をランダムに決定し、秘密鍵処理部４６０が受信端末Ｄの公開鍵で暗号化して、E_D［Session Key］を作成する。E_D［Session Key］はNonceの意味も兼ねることができるため、図３におけるNonceを削除し、代わりにE_D［Session Key］をその位置に置きかえる。秘密鍵処理部４６０が、Session Keyを用いて対称鍵暗号の出力（疑似乱数系列）を得る。演算部４７０が、送信端末一時アドレスADD_S，受信端末アドレスADD_D，送信端末の証明書$Cert_S$及びデジタル署名Sig_S（全てのフィールドを対象とした署名）と上記疑似乱数系列との排他的論理和を計算する。送受信部４２６が、全体をRREQとしてブロードキャスト送信する。

【００４６】
RREQを受信した中継端末Ｔ１は、特定の長さを有するRREQはSからのRREQであると想定してSig$_S$の検証は行わず（この問題に対する対処は、後述する。）、図３と同様な処理をして転送する。中継端末も同様な処理をして、転送する。
【００４７】
中継端末Ｔ２からRREQを受信した受信端末Dは以下の処理を行う。
【００４８】
受信した被暗号化共通鍵E_D［Session Key］を自分の秘密鍵を用いて復号化して、共通鍵（Session Key）を得る。復号の結果得られたSession Keyを用いて、対称鍵暗号の出力（疑似乱数系列）を得る。得られた疑似乱数系列と秘匿されているフィールドとの排他的論理和を取ることによって、データを復元することができる。
【００４９】
返信の際には、受信端末Dの乱数発生部で新たに作成した疑似乱数系列（受信時の乱数系列とは異なる）を用いて再暗号化する。すなわち、新しい疑似乱数系列とADD_S，ADD_D，$Cert_S$，Sig_S，SigDとの排他的論理和を取る。従ってRREPのADD_S，ADD_D，$Cert_S$，Sig_Sには、SとDの乱数系列のマスクがそれぞれ施されていることになる。
【００５０】
中継端末Ｔ１，Ｔ２を経由して転送されたRREPを受信したSは以下の処理を行う。
【００５１】
自分宛のRREPであるかどうかを検証する際に、受信端末Dが設定した疑似乱数系列を外す。これまで、対称鍵暗号の利用モードについては特に言及しなかったが、疑似乱数系列を出力するには、CTRモードでの利用が一般的である。
【００５２】
図９にはCTRモードの概要を示している。Initialization Vector（以下IVと言う）は、送受信者間で秘密裏に共有できることが望ましい。カウンタ（以下ctと言う）は、送受信者間で同期する必要があり、同期外れの影響を減らすためには生値をパケットに付加して伝送することが望ましい。
【００５３】
図１０は、図８において対称鍵暗号の利用モードにCTRモードを想定した例である。図５と異なる処理を中心に以下に説明する。
【００５４】
IVはSession Keyと連接して（以下”||”の記号で表示する）送信することとし、Seed＝Session Key || Ivとする。ctは、送信端末Sと受信端末Dで独立に選べるようにし（各々ct_S，ct_Dとする）、パケットの先頭にこのフィールドを付加する。なおctがインクリメンタルに連続するとパケットの順序が第三者に漏れるため、送信者はランダムな値を割り当てることとする。またctはNonceの意味合いも含むため、今までED［Session Key］をNonceとして捉えていたが、以下ではctがNonceの役割を果たすものとする。
【実施例３】
【００５５】
図１１及び１２を参照しながら、本発明の実施例３について説明する。図１１は、図１０と同様な図であるが、第三者に露呈される中継端末（ノード）に関する情報を網掛けで示している。中継情報の必要性について改めて考えると、送信端末Sと受信端末DはSource Routingを行うため全ての中継端末の情報を知る必要があるが、中継端末自体は以下の判断ができれば十分である。
【００５６】
１．RREQに対しては、自分宛であるかの確認、直前の中継端末からの情報の正当性。
【００５７】
２．RREPに対しては、転送アドレスリストに自分が含まれるかどうか。
【００５８】
従って不必要な情報の露呈は攻撃の材料となる危険性があるため、中継端末の情報に関

しても可能な限り、送信端末Sと受信端末Dにしか分からないように隠蔽するのが望ましい。そこで、以下ではプライバシーの向上のために、図１１の網掛けフィールドをSとDにしか分からないように隠蔽する例について説明する。

【００５９】

図１２は、図１１の網掛けフィールドを隠蔽するために、RREQでは一時公開鍵を適用し、RREPでは対称鍵暗号の対象を拡大した例を示す。図８，図１０と異なる処理を中心に以下に説明する。

【００６０】

送信端末Sの乱数発生部４３０が、RREQの送信に当たり、一時公開鍵（Ｋ＋）と一時秘密鍵（Ｋ－）のペアをランダムに決定する。一時公開鍵Ｋ＋と一時秘密鍵Ｋ－とをRREQに追加して送信するが、一時秘密鍵Ｋ－のみ疑似乱数系列の排他的論理和の対象とする。

【００６１】

RREQを受信した中継端末Ｔ２が、自分より以前の中継端末の情報（この場合ADD_{T1}，$Cert_{T1}$，Sig_{T1}）をＫ＋を用いて累積暗号化する。累積暗号化することによって、悪意のある中継端末が自分より以前の中継端末情報を逆順序で省略していった場合でも、受信端末Dで検出不可能となることを避けることができる。

【００６２】

RREQを受信した受信端末Dは、以下の処理を行う。

【００６３】

中継経路毎のSigを検証する。Sig_{T2}を検証した後、ADD_{T2}，$Cert_{T2}$，Sig_{T2}を除去する。中継端末の情報全体を一時秘密鍵Ｋ－を用いて復号する。Sig_{T1}を検証する。ADD_{T1}，$Cert_{T1}$，Sig_{T1}を除去する。Sig_Sを検証する。

【００６４】

一般的には、次の一連の処理を中継端末情報全体の長さから推測される中継回数だけ繰り返すことになる。すなわち、一時秘密鍵Ｋ－で復号、最外側のSigの検証及び最外側の付加情報の除去の一連の処理である。

【００６５】

受信端末Ｄが返信する際に、RREQからコピーした全ての情報に対して、受信端末Dで新たに作成した疑似乱数系列（受信時の乱数系列とは異なる）との排他的論理和を取って再暗号化し、RREPを作成する。マスクパタンの対象領域が拡大され、Ｋ－，Ｋ＋，E_D［Seed］，ADD_{T1}，$Cert_{T1}$，Sig_{T1}，ADD_{T2}，$Cert_{T2}$，Sig_{T2}にもマスクパタンが掛かることになる。

【００６６】

RREQからコピーした全ての情報にマスクパタンが掛けられているので、ADD_{T1}とADD_{T2}は隠蔽されており、中継端末において識別不可能となる。そこで、ADD_{T1}とADD_{T2}の生値を新設された中継アドレスリストフィールドに格納する。

【００６７】

RREP信号を受信した送信端末Sは、以下の処理を行う。

【００６８】

受信した被暗号化共通鍵E_D［Seed］を復号化して、検証する。中継アドレスリストに自分のアドレスADD_Sを発見できないため、乱数系列を外す。ADD_S，ADD_D，Seed、$Cert_S$，Sig_Sの組み合わせから、自分が以前に送信したRREQに対する応答であることを認識する。Sig_Dを検証する。中継経路毎のSigを検証する。すなわち、RREPをRREQに置きかえてSig_Dを除去する。Sig_{T2}を検証した後、ADD_{T2}，$Cert_{T2}$，Sig_{T2}を除去する。Sig_{T1}を検証した後、ADD_{T1}，$Cert_{T1}$，Sig_{T1}を除去する。中継経路情報（S→Ｔ１→Ｔ２→D）を確定する。

【実施例４】

【００６９】

図１３及び図１４を参照しながら、本発明の実施例４について説明する。図１３は、図１２と同様な図であるが、第三者に露呈される中継端末（ノード）に関する情報を網掛けで示している。中継端末のアドレスに関しても可能な限り、送信端末Sと受信端末Dと中継

端末自身にしか分からないように隠蔽することが望ましい。そこで、プライバシーの向上のために、図１３の網掛けフィールドを送信端末Sと受信端末Dと中継端末自身にしか分からないように隠蔽する実施例を説明する。

【００７０】

簡単な対処としては、ADD_{T1}，ADD_{T2}を一時アドレスにする方法があるが、この方法だけでは複数のパケットを通じてしばらく同じ中継アドレスが適用されてしまうため、パケットの関連性が露呈する危険性が存在する。従って、パケット毎に異なる一時アドレスが適用される方が、よりプライバシーの漏洩に強い仕組みができあがる。この問題に対処するために、一時公開鍵とハッシュ関数の活用を考える。

【００７１】

図１４は図１３の網掛けフィールドを隠蔽するために、RREQでは乱数を一時公開鍵で暗号化し、RREPでは乱数にハッシュ関数を適用した例である。図９とは異なる処理を中心に以下に説明する。なお、$rand_X$とは端末Xで決定した乱数、h（y）とはyのハッシュ値を意味している。ハッシュ関数とは、ドキュメントや数字などの文字列の羅列から一定長のデータに要約するためのある関数・手順のことをいう。関数を通して出力される値は、「ハッシュ値」と呼ばれる。“SHA-1”と“MD5”というハッシュ関数が代表的で、いずれも1方向関数であるため、生成データから原文を推定することは不可能である。通信回線を通じてデータを送受信する際に、経路の両端でデータのハッシュ値を求めて両者を比較すれば、データが通信途中で改ざんされていないかを調べることができる。

【００７２】

RREQを受信した中継端末Ｔ１は、自己のアドレスADD_{T1}の代わりに$E_{K+}[rand_{T1}]$を設定する。

【００７３】

Ｔ２もＴ１と同様の処理を行う。

【００７４】

RREQを受信したDは、$rand_{T1}$，$rand_{T2}$を取得し、ADD_{T1}，ADD_{T2}の生値の代わりに、$h(rand_{T1}||ct_D)$，$h(rand_{T2}||ct_D)$を適用する。

【００７５】

RREPを受信したＴ２は、自分のアドレスを$h(rand_{T2}||ct_D)$として認識する。

【００７６】

Ｔ１もＴ２と同様の処理を行う。

【００７７】

RREPを受信した送信端末Sは以下の処理を行う。

【００７８】

中継アドレスリストで自分のアドレスを発見する際、$h(rand_S||ct_D)$を検査する。$rand_{T1}$，$rand_{T2}$を取得する。

【実施例５】

【００７９】

図１４乃至図１６を参照しながら、本発明の実施例５について説明する。

【００８０】

図１４を参照すると、RREQのパケット長やRREPの中継アドレスリストから、送信端末Sと受信端末Dに関する情報が以下のように漏れる危険性が高いことが分かる。

【００８１】

・RREQ：パケット長から、中継端末Ｔ１が受信端末Sの隣にいることが分かる。

【００８２】

・RREP：中継端末Ｔ１と中継端末Ｔ２が結託（共謀）すれば、中継アドレスリストから、受信端末Dは中継端末Ｔ２の隣（SはＴ１の隣）であることが分かる。そこで、ダミー情報（乱数）を活用して送信端末S及び受信端末Dに中継端末であるかのように振る舞わせることにより、送信端末Sと受信端末Dの情報を可能な限り隠蔽する例を説明する。

【００８３】

図１５は、送信端末SからのRREQ信号及び受信端末DからのRREP信号の各々に、ダミー情報を付与して、両端末があたかも中継端末であるかのように振る舞わせたものである。前述の例とは異なる処理を中心に以下に説明する。　送信端末Sは、RREQ信号中にダミーの中継端末情報（図１５では１中継分を意味するDummy1，Dummy2）を付与する。ダミー情報が存在するために、送信端末Ｓの情報が露呈していても、第三者から見て、発信端末と中継端末との区別がつかない。

【００８４】

RREQ信号を受信した中継端末Ｔ１は、Sig_Sの検証を行う。直前上記の例ではSig_Sの検証ができなかったので、特定の長さのRREQはSからのRREQであると想定してSig_Sの検証は行わなかった。本実施例では、Sが中継端末のふりをするため証明書$Cert_S$を明かせるようになり、認証が可能になった。

【００８５】

RREQを受信したDは以下の処理を行う。

【００８６】

一時秘密鍵Ｋ－を用いて復号化し、中継経路毎のSigを再外側から順番に検証していき、$Cert_S$が出現するまで検証処理を繰り返す。直前上記の例では中継ノード情報全体の長さから推測される中継回数だけ処理を繰り返していたが、本実施例では、Sが中継端末のふりをするため、その方法は適用できない。

【００８７】

受信端末Ｄにおいて、RREP信号の中継アドレスリストに、ダミーアドレス（図１５では２つ分のDummyADD1，　DummyADD2）を付加し、疑似乱数系列との排他的論理和を取る。

【００８８】

RREP信号を受信した送信端末Ｓは、中継経路毎のSigの検証を送信端末Dと同様に行う。

【００８９】

ここで、図１５を良く見ると、RREP信号のパケット長さから、中継段数に関する情報が漏れる危険性があることが分かる。そもそもRREP信号の内容は送信端末Ｓ及び受信端末Ｄだけが認識できれば十分であり、第三者が識別をする必要はない。そこで、RREP信号の素性を可能な限り隠蔽する例について以下に説明する。

【００９０】

図１６は、RREPの素性を可能な限り隠蔽した例である。前述の例と異なる処理を中心に以下に説明する。

【００９１】

受信端末Dは、RREP信号の作成にあたり、以下の処理を行う。

【００９２】

RREPの代わりに、送信端末ＳのみがRREPかDataかを判別できる第２の識別フィールド（RREP／Data）を追加する。ダミー情報（乱数）のパディングを追加する（図１６におけるDummy Padding）。Lengthフィールドを追加して、Dummy Paddingを除く長さを設定する。第２の識別フィールド、Dummy Padding、Lengthの３つには、受信端末Dが設定したマスクパタンをかける。

【００９３】

RREP／Dataを受信した送信端末Ｓは、受信端末Dが設定したマスクパタンを外した後に、以下の処理を行う。

【００９４】

１．第２の識別フィールドからRREPであることを認識する。

【００９５】

２．Lengthフィールドを考慮して、Dummy Paddingを除去する。

【実施例６】

【００９６】

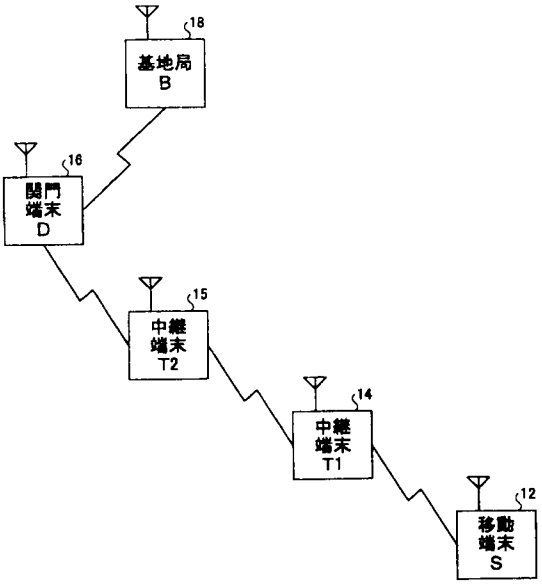
図１７に本発明の実施例６を示す。図１７に示す実施例６は、上記実施例を全て含んだ態様の例である。従って、説明を省略する。

【実施例７】
【００９７】
次に、仮にＴ２が悪意のある中継端末であるとすると、中継端末Ｔ２が中継端末Ｔ１の情報を故意に破棄してしまうことがあり得る。そこで、そのような悪事に対処するための例について以下に説明する。
【００９８】
図１７を参照して説明する。中継端末Ｔ１の情報とその直前の端末Dummy2の情報とに不可分な関連を持たせることで、中継端末Ｔ１の情報が破棄されたことを見破る仕組みを考える。
【００９９】
図１８に示すように、中継端末Ｔ１において、その直前の端末であるDummy2の情報に対して、中継端末T1の情報に基づく$K_{T1} = h(rand_{T1}, Cert_{T1})$を鍵とするブロック暗号による暗号化を施す。$rand_{T1}$とは端末Ｔ１で決定した乱数、$Cert_{T1}$は、証明書発行部が発行する端末Ｔ１の証明書であり、h（y）とはyのハッシュ値を意味している。
【０１００】
中継端末Ｔ２においても、その直前の端末であるＴ１の情報に対して、中継端末T2の情報に基づく$K_{T2} = h(rand_{T2}, Cert_{T2})$を鍵とするブロック暗号による暗号化を施す。従って、この暗号化を復元するには、受信端末Dは、正しい中継端末情報を知る必要がある。
【０１０１】
Dummyを用いた場合を例にとり本実施例を説明したが、本実施例に係る発明は実存する中継端末に関しても応用可能であり、それ以外の多種多様な構成に対しても応用可能である。直前の端末情報に限らず上流の任意の端末情報を暗号化しても良い。
【０１０２】
上記のような構成を備えることによって、もし悪意のある中継端末が上流の中継端末の情報を故意に破棄したとしても、受信端末Ｄにおいて、破棄された中継端末直前の端末の情報が正しく復号されないことになる。こうして受信端末Ｄは、この偽造経路を見破ることができる。
【０１０３】
このように、本実施例によれば、中継端末による処理負荷をそれほど大きくすることなく、悪意の中継端末による中継端末情報の偽造を防止することができ、偽造不可能なように経路情報を隠蔽可能であり、第三者に対する送受信者のプライバシーが向上される。
【産業上の利用可能性】
【０１０４】
本発明に従った、通信端末及びアドホックネットワーク経路制御方法は、秘匿が要求される無線又は有線通信分野において利用することができる。
【図面の簡単な説明】
【０１０５】
【図１】従来のアドホックネットワークの概略を示す概念図である。
【図２】従来のアドホックネットワーク構築可能な移動端末の概略ブロック図である。
【図３】従来のアドホックネットワーク構築のための経路制御信号のデータを示すチャートである。
【図４】本発明の実施例に従った移動端末のブロック図である。
【図５】実施例１に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートである。
【図６】実施例２を説明するための経路制御信号のデータを示すチャートであり、第三者への送受信端末の露呈が示されている。
【図７】実施例２に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ADDSに一時アドレスを使用している。
【図８】実施例２に従った、アドホックネットワーク構築のための経路制御信号のデータ

を示すチャートであり、ハイブリッド暗号を使用している。
【図９】実施例２に従った、ＣＴＲモードの概要を示す概念図である。
【図１０】実施例２に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ＣＴＲモードを使用している。
【図１１】実施例３を説明するための経路制御信号のデータを示すチャートであり、第三者への中継情報の露呈が示されている。
【図１２】実施例３に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、一時公開鍵を使用している。
【図１３】実施例４を説明するための経路制御信号のデータを示すチャートであり、第三者への中継端末アドレスの露呈が示されている。
【図１４】実施例４に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ハッシュ関数の利用を示している。
【図１５】実施例５に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ダミー情報が付加されている。
【図１６】実施例５に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、RREPの素性を可能な限り隠蔽した例である。
【図１７】各実施例の全て含んだ、アドホックネットワーク構築のための経路制御信号のデータを示すチャートである。
【図１８】実施例７に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、中継端末の破棄を防止する例である。
【符号の説明】
【０１０６】
４００　移動端末
４２２　リクエスト／リプライ発生部
４２４　制御部
４２６　送受信部
４２７　アドレス記憶部
４２８　アドレス比較部
４３０　乱数発生部
４４０　証明書発行部
４５０　デジタル署名作成部
４６０　秘密鍵処理部
４７０　演算部
４８０　検証部

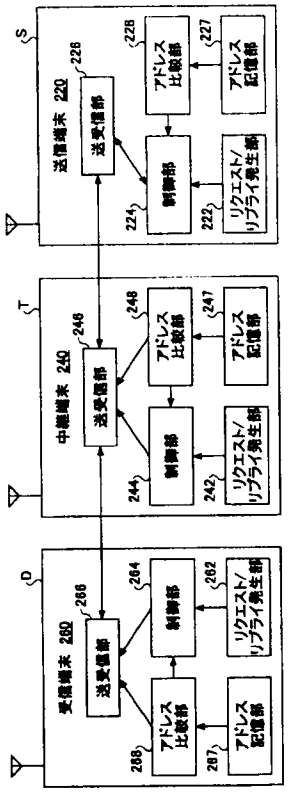
【図１】

従来のアドホックネットワークの概略を示す概念図



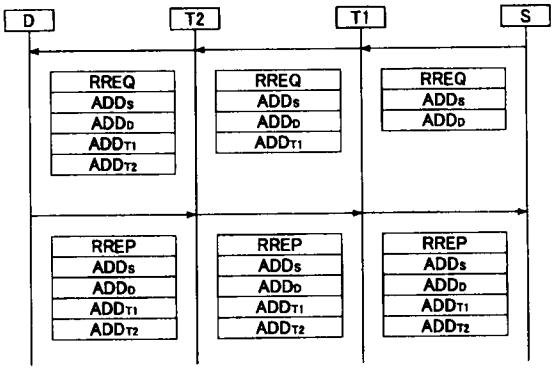
【図２】

従来のアドホックネットワーク構築可能な移動端末の概略ブロック図



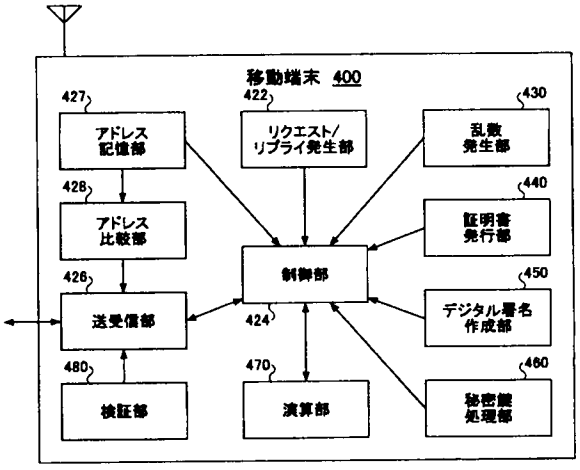
【図３】

従来のアドホックネットワーク構築のための経路制御信号のデータを示すチャート



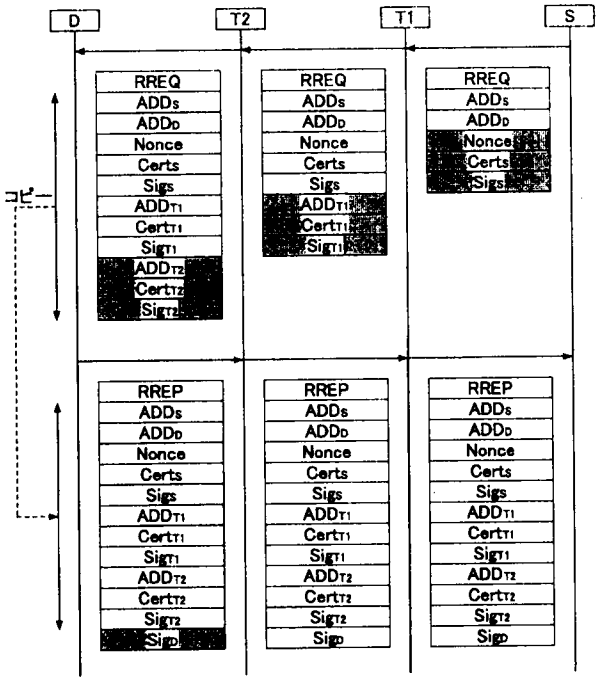
【図４】

本発明の実施例に従った移動端末のブロック図



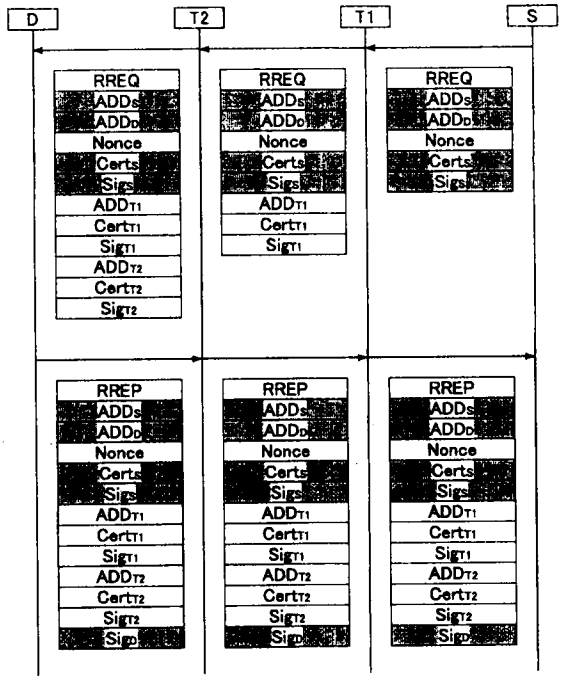
【図５】

実施例1に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャート



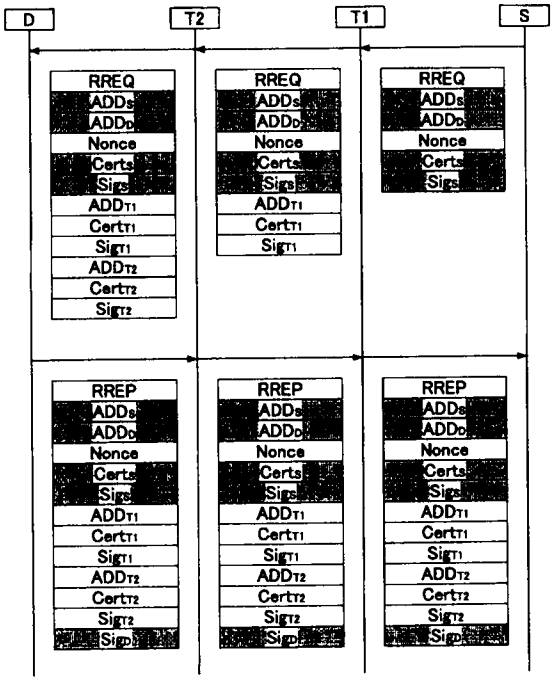
【図６】

実施例2を説明するための経路制御信号のデータを示すチャートであり、第三者への送受信端末の露呈が示されている図



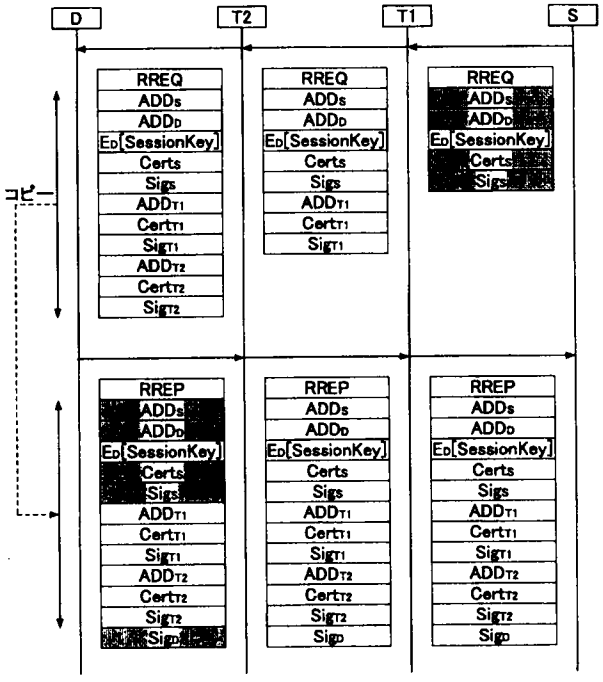
【図７】

実施例2に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ADDSに一時アドレスを使用している図



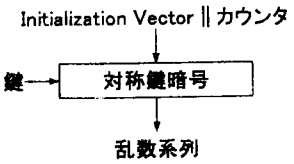
【図８】

実施例2に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ハイブリッド暗号を使用している図



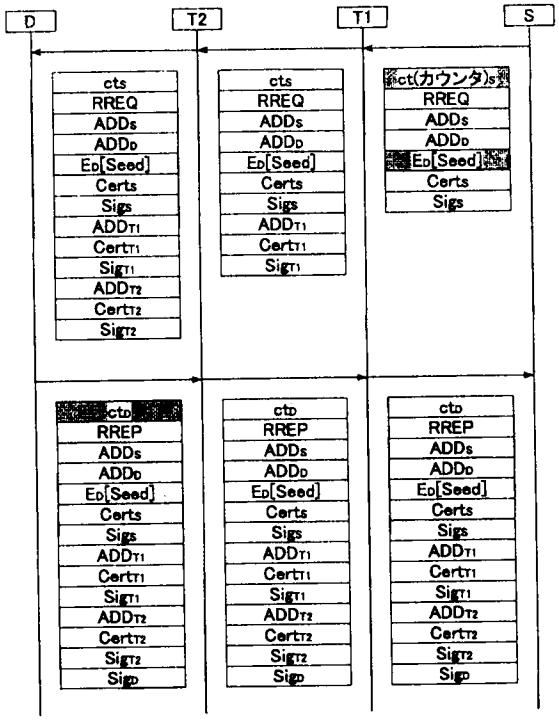
【図９】

実施例2に従った、CTRモードの概要を示す概念図



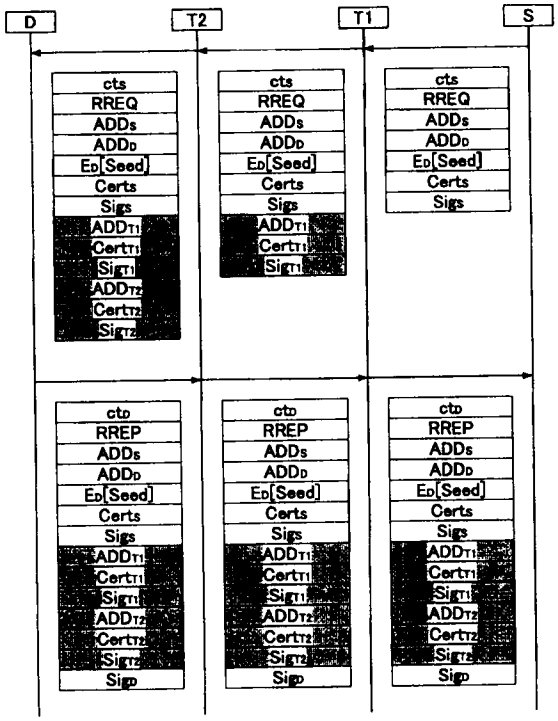
【図１０】

実施例2に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、CTRモードを使用している図



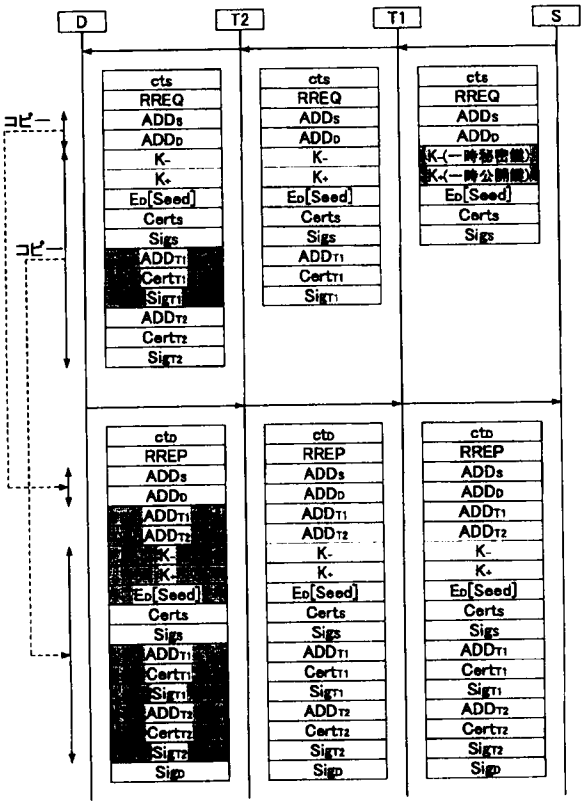
【図１１】

実施例3を説明するための経路制御信号のデータを示すチャートであり、第三者への中継情報の露呈が示されている図



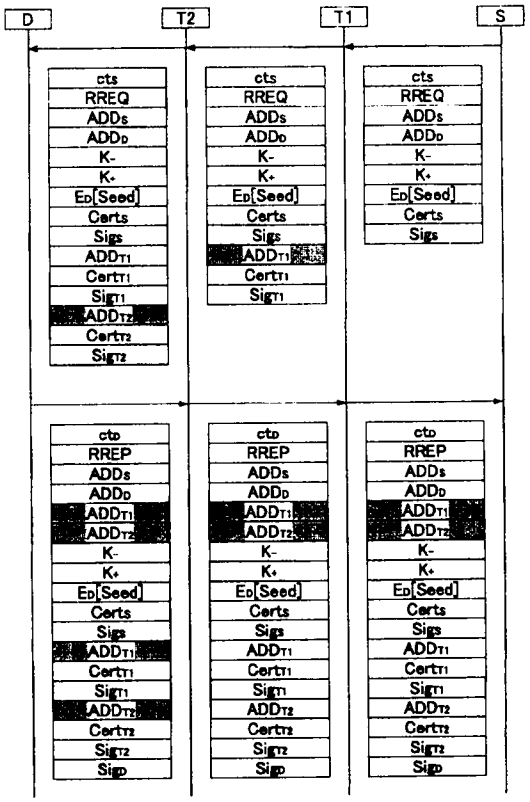
【図１２】

実施例3に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、一時公開鍵を使用している図



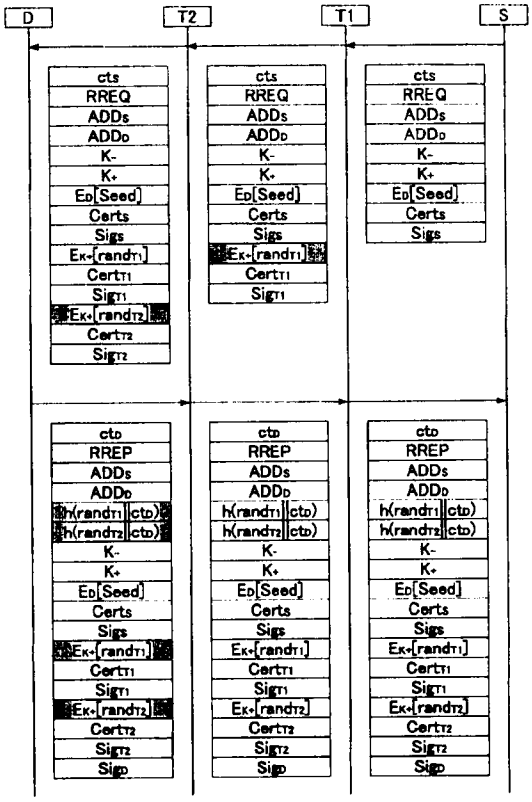
【図１３】

実施例4を説明するための経路制御信号のデータを示すチャートであり、第三者への中継端末アドレスの露呈が示されている図



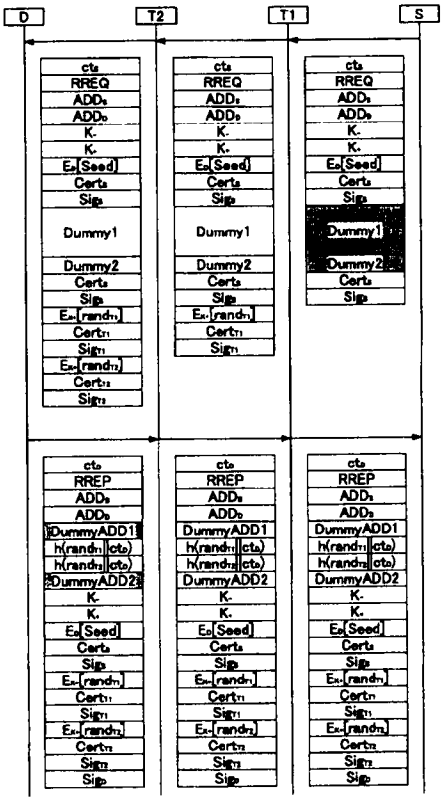
【図１４】

実施例4に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ハッシュ関数の利用を示している図



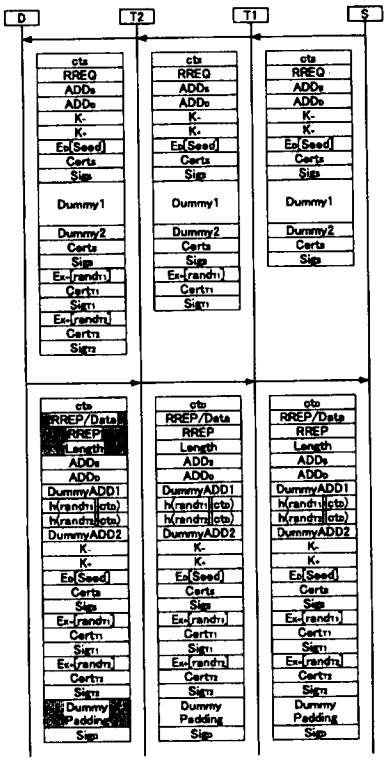
【図１５】

実施例5に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、ダミー情報が付加されている図



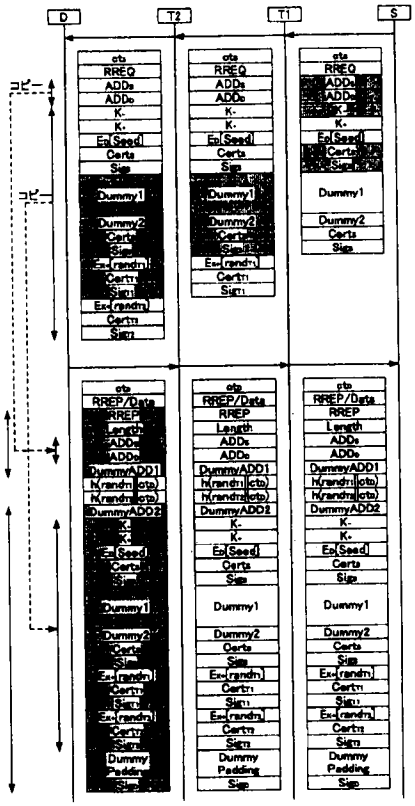
【図１６】

実施例5に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、RREPの素性を可能な限り隠蔽した例



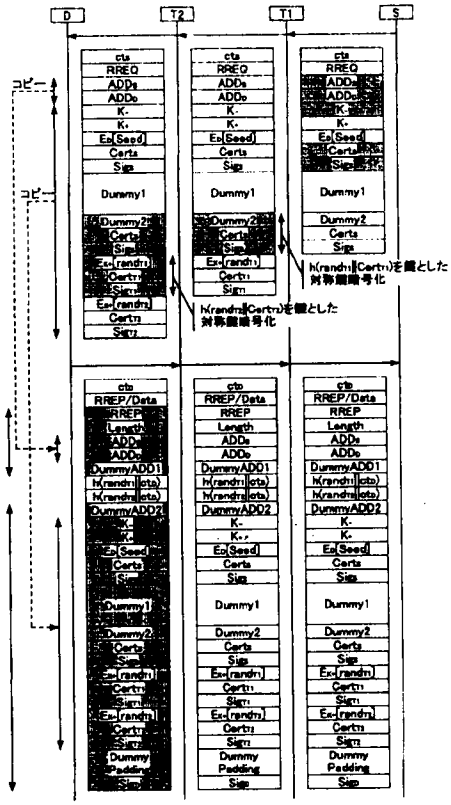
【図１７】

各実施例の全て含んだ、アドホックネットワーク構築のための経路制御信号のデータを示すチャート



【図１８】

実施例7に従った、アドホックネットワーク構築のための経路制御信号のデータを示すチャートであり、中継端末の破棄を防止する例



フロントページの続き

Fターム(参考) 5K033 AA09 CB01 DA05 DA19 DB18 EC03